Basics of Computer Networking

Last Updated : 15 Feb, 2025

A computer network is a collection of interconnected devices that share resources and information. These devices can include computers, servers, printers, and other hardware. Networks allow for the efficient exchange of data, enabling various applications such as email, file sharing, and internet browsing.

Basic Terminologies of Computer Networks

- **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
- **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and other devices.
- **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.
- **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.
- **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.

- **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.

- **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.

- **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

How Does a Computer Network Work?

Basics building blocks of a Computer network are Nodes and Links. A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more. Link in Computer Networks can be defined as wires or cables or free space of wireless networks.

The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an IP Address, that helps in identifying a device.

What do Computer Networks do?

Computer networks first developed in 1950 for military and defense purpose. At that time they are mainly used to send data through telephone lines and had limited use in business or science.

Today computer networks are essential for businesses also. Modern networks offer more than just connecting devices. They play a key role in helping businesses adapt to the digital world and succeed. These networks have become more flexible, automated, and secure, making them even more important in today's business environment.

Modern computer networks can:

- **Work Virtually:** The physical network can be divided into smaller virtual networks. In these virtual networks, devices are connected and can send data through multiple physical routes. For example, many business networks use the internet this way.

- **Connect on a Large Scale:** Modern networks link many smaller, spread-out networks into one big, powerful system. Automation and monitoring tools help manage and adjust the network as needed, allowing it to grow or shrink based on demand.

- **Adapt Quickly:** Many networks are controlled by software, so changes can be made quickly through a digital dashboard. This allows traffic to be managed easily.

- **Keep Data Secure:** Built-in security features like encryption and access control protect data. Additional protections like antivirus software, firewalls, and malware protection can be added to strengthen network security.

Types of Enterprise Computer Networks

- **LAN:** A Local Area Network (LAN) is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.

- **WAN:** A Wide Area Network (WAN) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.

- **Cloud Networks:** Cloud Networks can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

These are just a few basic concepts of computer networking. Networking is a vast and complex field, and there are many more concepts and technologies involved in building and maintaining networks. Now we are going to discuss some more concepts on Computer Networking.

- **Open system:** A system that is connected to the network and is ready for communication.
- **Closed system:** A system that is not connected to the network and can't be communicated with.

Types of Computer Network Architecture

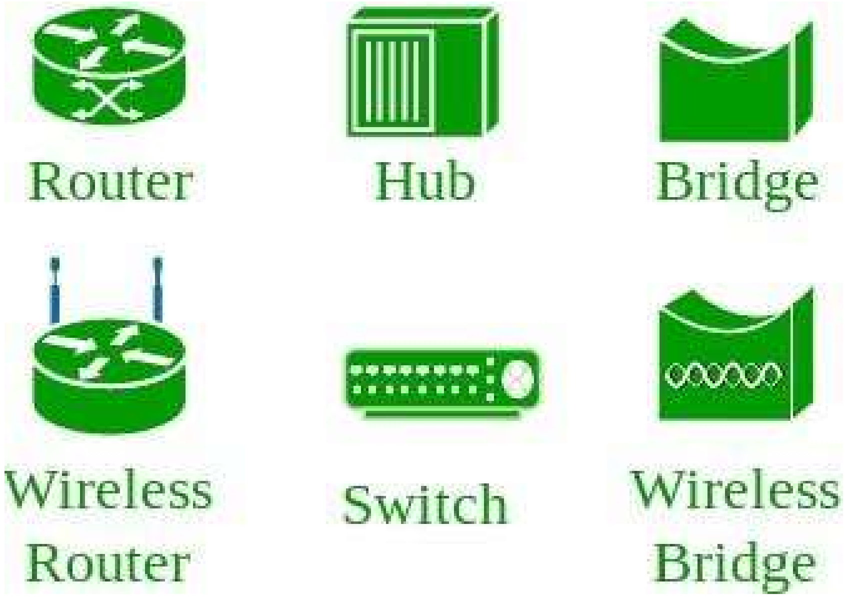
Computer Network falls under these broad Categories:

- **Client-Server Architecture:** Client-Server Architecture is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behaviour.

- **Peer-to-Peer Architecture:** In P2P (Peer-to-Peer) Architecture, there is not any concept of a Central Server. Each device is free for working as either client or server.

Network Devices

An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.



Network Devices

Network Topology

The Network Topology is the layout arrangement of the different devices in a network. Some types of network topologies are:

- **Bus Topology:** In **bus topology** all devices are connected to a single central cable called a bus. Data is sent along this cable and all devices share the same connection. Simple and cheap to set up but if the main cable fails the whole network goes down.

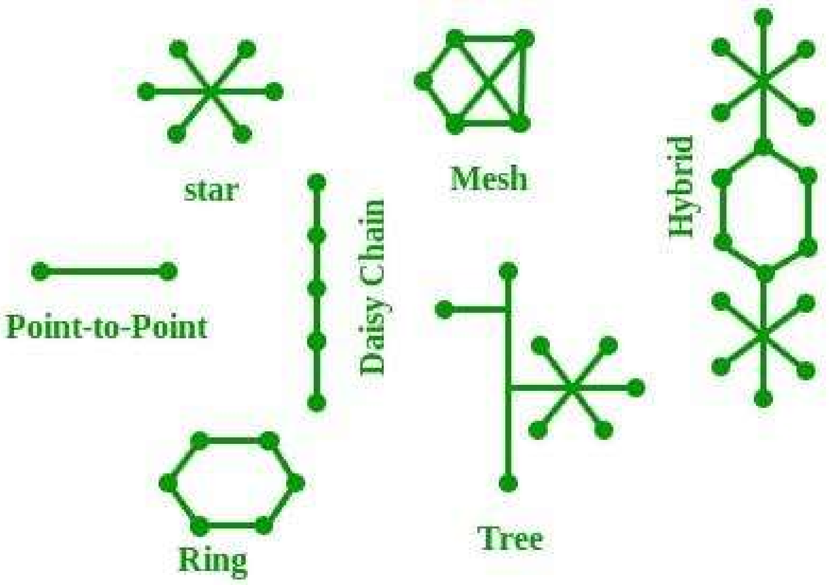
- **Star Topology:** In **star topology** all devices are connected to a central node called hub or switch. The hub controls the flow of data between devices. If one device fails the rest of the network is unaffected. But, if the central hub fails the whole network stops working.

- **Ring Topology**: In ring topology devices are connected in a circular loop with each device connected to two others. Data travels in one direction (or sometimes both) passing through each device until it reaches its destination. A failure in one device can affect the whole network.

- **Mesh Topology**: In mesh topology every device is connected to every other device in the network. It provides multiple paths for data so if one path fails another can take over.

- **Tree Topology**: Tree topology is the combination of star and bus topology. Tree topology is good for organizing large networks and allows for easy expansion.

- **Hybrid Topology**: Hybrid topology is the combination of two or more different topologies (like star and mesh). It is flexible and can be customized based on the network's specific needs.



Network Topology

OSI Model

OSI stands for Open Systems Interconnection. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer. The OSI has been developed by the International Organization For Standardization and it is 7 layer architecture. Each layer of OSI has different functions and each layer has to follow different protocols. The 7 layers are as follows:

- Physical Layer
- Data link Layer
- Network Layer

- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

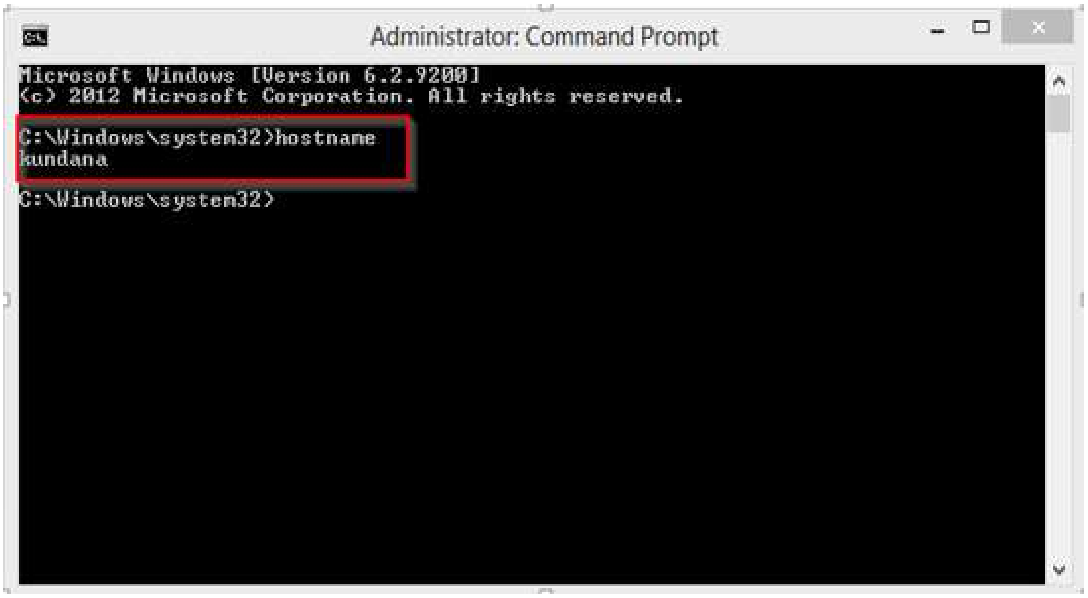
Network Protocols

A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists a different protocol defined at each layer of the OSI model. A few such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

- **Transmission Control Protocol/Internet Protocol (TCP/IP):** TCP/IP is the foundational protocol suite of the internet, enabling reliable communication. TCP Ensures data is delivered reliably and in order and IP routes data packets to their destination based on IP addresses.
- **Hypertext Transfer Protocol (HTTP) and HTTPS:** HTTP and HTTPS protocols used for transmitting web pages. **In HTTP** communication is unsecured and in **HTTPS** secured communication using SSL/TLS encryption.
- **Simple Mail Transfer Protocol (SMTP):** SMTP protocol used to send email. SMTP protocol works with other protocols like POP3 and IMAP for email retrieval.
- **File Transfer Protocol (FTP):** FTP protocol used for transferring files between computers. Includes commands for uploading, downloading, and managing files on a remote server.
- **Dynamic Host Configuration Protocol (DHCP):** DHCP protocol automatically assigns IP addresses to devices on a network. Reduces manual configuration and IP address conflicts.
- **Domain Name System (DNS):** DNS Translates human-friendly domain names into IP addresses. Ensures seamless navigation on the internet.

Unique Identifiers of Network

Hostname: Each device in the network is associated with a unique device name known as Hostname. Type “hostname” in the command prompt(Administrator Mode) and press ‘Enter’, this displays the hostname of your machine.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
kundana

C:\Windows\system32>
```

HostName

IP Address (Internet Protocol address): Also known as the Logical Address, the IP Address is the network address of the system across the network. To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet. The length of an IPv4 address is 32 bits, hence, we have 2^{32} IP addresses available. The length of an IPv6 address is 128 bits.

In **Windows** Type “ipconfig” in the command prompt and press ‘Enter’, this gives us the IP address of the device. For **Linux,** Type “ifconfig” in the terminal and press ‘Enter’ this gives us the IP address of the device.

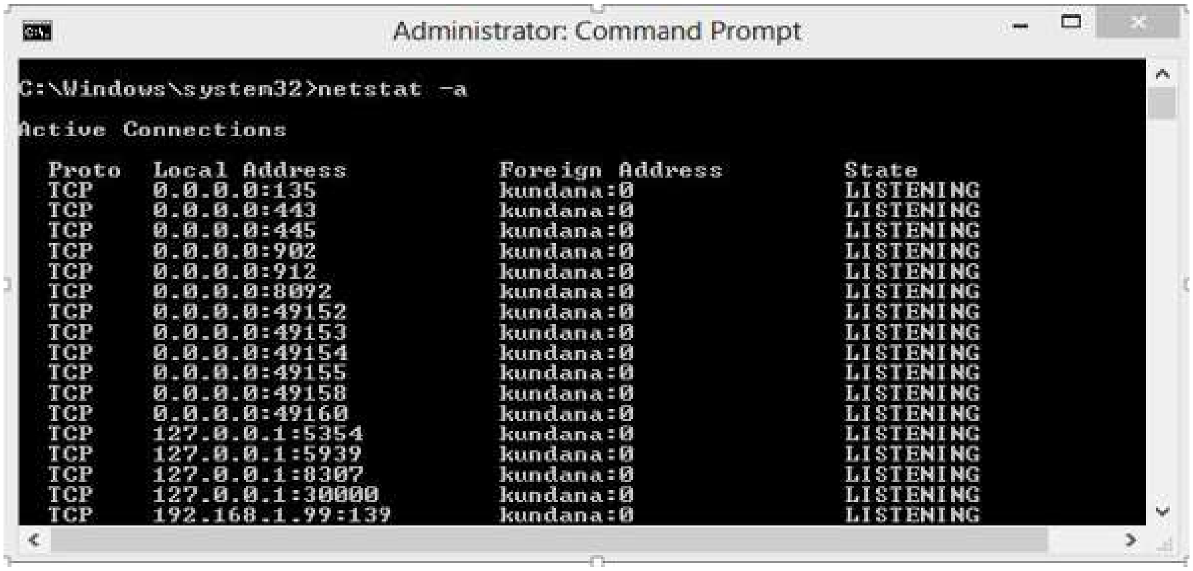
MAC Address (Media Access Control address): Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card). A MAC address is assigned to the NIC at the time of manufacturing. The length of the MAC address is: 12-nibble/ 6 bytes/ 48 bits Type “ipconfig/all” in the command prompt and press ‘Enter’, this gives us the MAC address.

Port: A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

A port number is a 16-bit integer, hence, we have 2^{16} ports available which are categorized as shown below:

Port Types	Range
Well known Ports	0 – 1023
Registered Ports	1024 – 49151
Ephemeral Ports	49152 - 65535

Number of ports: 65,536
Range: 0 – 65535
Type “**netstat -a**” in the command prompt and press ‘Enter’, this lists all the ports being used.



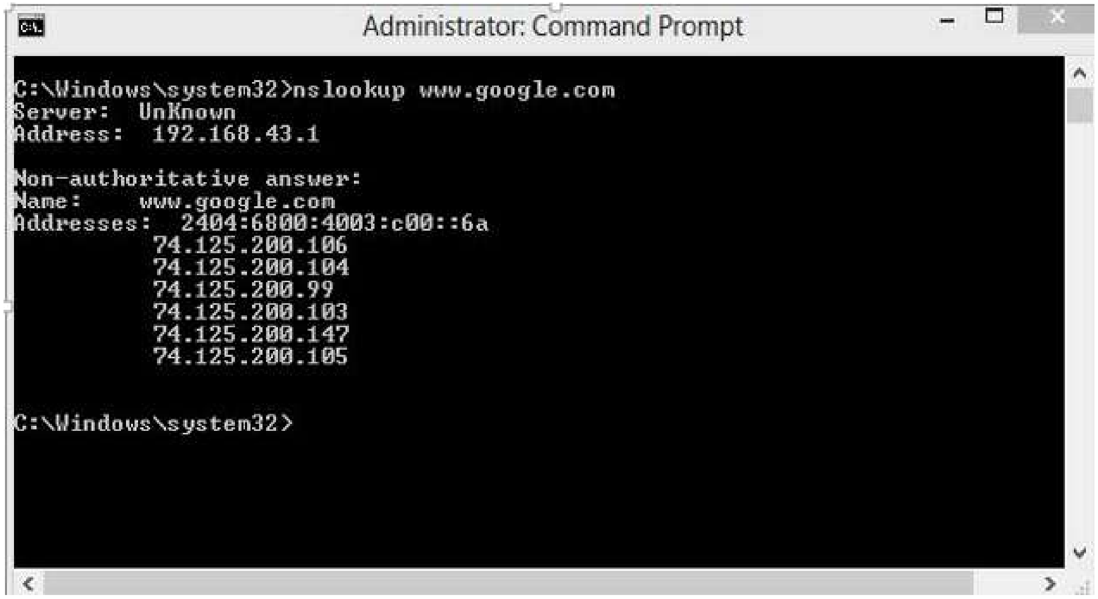
```
C:\Windows\system32>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            kundana:0              LISTENING
  TCP    0.0.0.0:443            kundana:0              LISTENING
  TCP    0.0.0.0:445            kundana:0              LISTENING
  TCP    0.0.0.0:902            kundana:0              LISTENING
  TCP    0.0.0.0:912            kundana:0              LISTENING
  TCP    0.0.0.0:8092           kundana:0              LISTENING
  TCP    0.0.0.0:49152          kundana:0              LISTENING
  TCP    0.0.0.0:49153          kundana:0              LISTENING
  TCP    0.0.0.0:49154          kundana:0              LISTENING
  TCP    0.0.0.0:49155          kundana:0              LISTENING
  TCP    0.0.0.0:49158          kundana:0              LISTENING
  TCP    0.0.0.0:49160          kundana:0              LISTENING
  TCP    127.0.0.1:5354         kundana:0              LISTENING
  TCP    127.0.0.1:5939         kundana:0              LISTENING
  TCP    127.0.0.1:8307         kundana:0              LISTENING
  TCP    127.0.0.1:30000        kundana:0              LISTENING
  TCP    192.168.1.99:139       kundana:0              LISTENING
```

List of Ports

Socket: The unique combination of IP address and Port number together is termed a Socket.

Other Related Concepts

DNS Server: DNS stands for **Domain Name System**. DNS is basically a server that translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don't have to remember all the IP addresses of each and every website. The command '**nslookup**' gives you the IP address of the domain you are looking for. This also provides information on our DNS Server. \



```
C:\Windows\system32>nslookup www.google.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4003:c00::6a
          74.125.200.106
          74.125.200.104
          74.125.200.99
          74.125.200.103
          74.125.200.147
          74.125.200.105


C:\Windows\system32>
```

Domain IP Address

ARP: ARP stands for **Address Resolution Protocol**. It is used to convert an IP address to its corresponding physical address(i.e., MAC Address). ARP is used by the Data Link Layer to identify the MAC address of the Receiver's machine.

RARP: RARP stands for **Reverse Address Resolution Protocol**. As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

The Domain Name System (DNS) is a critical component of computer networking. It converts easily recognizable domain names, such as www.example.com, into numerical IP addresses that computers use to identify each other on the network.

How DNS Works?

DNS works efficiently, translating user-friendly domain names into IP addresses, allowing seamless navigation on the internet. Below step by step working of DNS:

- **User Input:** When a user enters a domain name in a browser, the system needs to find its IP address.
- **DNS Query:** The user's device sends a DNS query to the DNS resolver.
- **Resolver Request:** The DNS resolver checks its cache for the IP address. If not found, it forwards the request to the root DNS server.
- **Root DNS Server:** The root DNS server provides the address of the TLD (Top-Level Domain) server for the specific domain extension (e.g., .com).
- **TLD DNS Server:** The TLD server directs the resolver to the authoritative DNS server for the actual domain.
- **Authoritative DNS Server:** The authoritative DNS server knows the IP address for the domain and provides it to the resolver.
- **Response to User:** The resolver stores the IP address in its cache and sends it to the user's device.
- **Access Website**: With the IP address, the user's device can access the desired website.

Network Security

Ensuring the security of a network is crucial to protect data and resources from unauthorized access and attacks. Key aspects of network security include:

- **Firewalls:** Devices or software that monitor and control incoming and outgoing network traffic based on security rules.
- **Encryption:** The process of encoding data to prevent unauthorized access. Commonly used in VPNs, HTTPS, and secure email.

- **Intrusion Detection Systems (IDS):** Tools that monitor network traffic for suspicious activity and potential threats.
- **Access Control:** Mechanisms that restrict access to network resources based on user identity and role.
- **Regular Updates and Patching:** Keeping software and hardware up to date to protect against vulnerabilities.

Why Use Computer Networks?

Computer network play a important role in modern life. Here are some key benefits of computer networks:

- **Fast and Easy Communication:** Networks enable all types of digital communication, like emails, messaging, file sharing, video calls, and streaming.

- **More Storage Space:** Suppose if we don't have a cloud storage then we have to store data in physical files that will consume a physical space so computer network provide a storage for storing data.

- **Easier Sharing of Information:** Networks make it simpler for users and teams to share resources and information. Teams can collaborate more easily, and users get faster response from network devices.

- **Better Security:** Well designed networks are more reliable and give businesses more options for keeping data safe. They come with built-in security features like encryption and access controls to protect sensitive information from cyber threats.

Conclusion

Understanding the basics of computer networking is essential in today's interconnected world. Networks enable the seamless exchange of information, support countless applications, and underpin the functionality of the internet. From different types of networks and their components to protocols and security measures, a solid grasp of these concepts is foundational for anyone working in or with technology. As technology evolves, so too will the complexity and capabilities of computer networks, making continuous learning and adaptation crucial.

Comment More info Advertise with us

Next Article

Types of Network Topology

Similar Reads

1. Challenges of Computer Network
2. Basic Characteristics of Computer Networks
3. Uses of Computer Network
4. Types of Computer Networks
5. TCP/IP in Computer Networking
6. Computer Networks | Set 14
7. Computer Network Tutorial
8. Computer Network - Cheat Sheet
9. Physical Components of Computer Network
10. Socket in Computer Network

Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Registered Address:
K 061, Tower K, Gulshan Vivante
Apartment, Sector 137, Noida, Gautam
Buddh Nagar, Uttar Pradesh, 201305

Types of Network Topology

Last Updated : 02 Apr, 2025

Network topology refers to the arrangement of different elements like nodes, links, or devices in a computer network. Common types of network topology include bus, star, ring, mesh, and tree topologies, each with its advantages and disadvantages. In this article, we will discuss different types of network topology in detail.

What is Network Topology?

Network topology is the way devices are connected in a network. It defines how these components are connected and how data transfer between the network. Understanding the different types of network topologies can help in choosing the right design for a specific network.

There are two major categories of Network Topology i.e. Physical Network topology and Logical Network Topology. Physical Network Topology refers to the actual structure of the physical medium for the transmission of data. Logical network Topology refers to the transmission of data between devices present in the network irrespective of the way devices are connected. The structure of the network is important for the proper functioning of the network. one must choose the most suitable topology as per their requirement.

Types of Network Topology

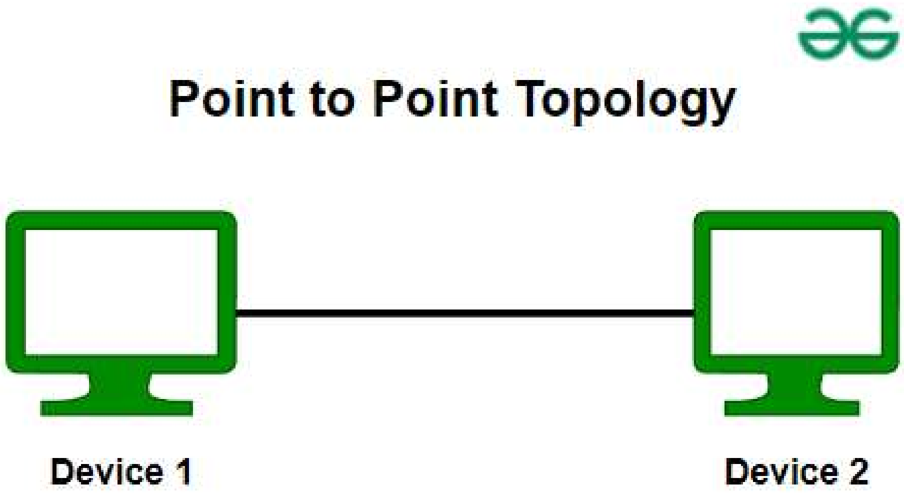
Below mentioned are the types of Network Topology

- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology

- Ring Topology
- Tree Topology
- Hybrid Topology

Point to Point Topology

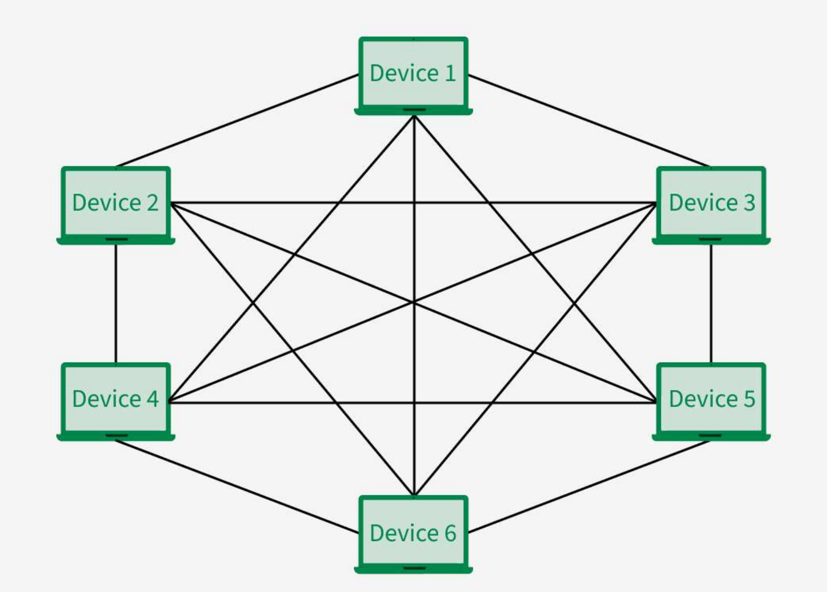
Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Point to Point Topology

Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. Every device is connected to another via dedicated channels. These channels are known as links. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



Mesh Topology

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure , there are 6 devices connected to each other, hence the total number of ports required by each device is 5. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is $^{N}C_{2}$ i.e. N(N-1)/2. In Figure, there are 6 devices connected to each other, hence the total number of links required is 6*5/2 = 15.

Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages of Mesh Topology

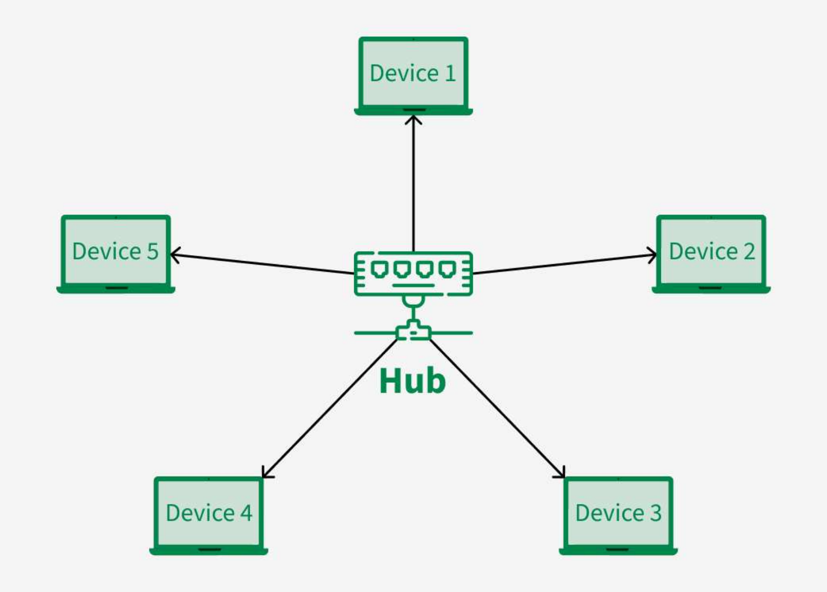
- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.

- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Star Topology

Advantages of Star Topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.

- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

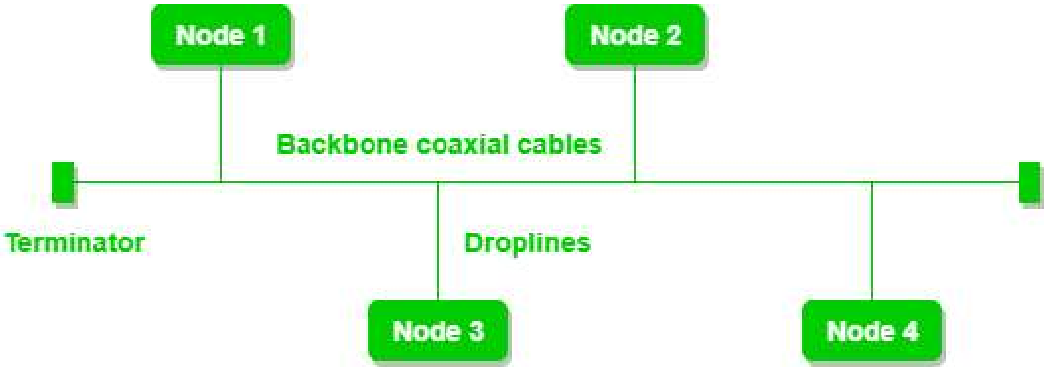
Disadvantages of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

A common example of star topology is a **local area network (LAN)** in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Bus Topology

Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

Disadvantages of Bus Topology

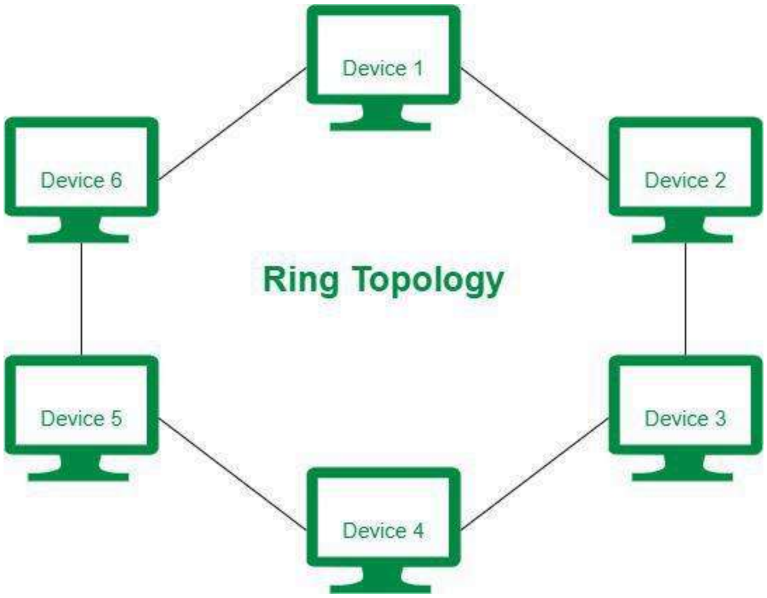
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



Ring Topology

The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Operations of Ring Topology

- One station is known as a **monitor** station which takes all the responsibility for performing the operations.
- To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
- When no station is transmitting the data, then the token will circulate in the ring.
- There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

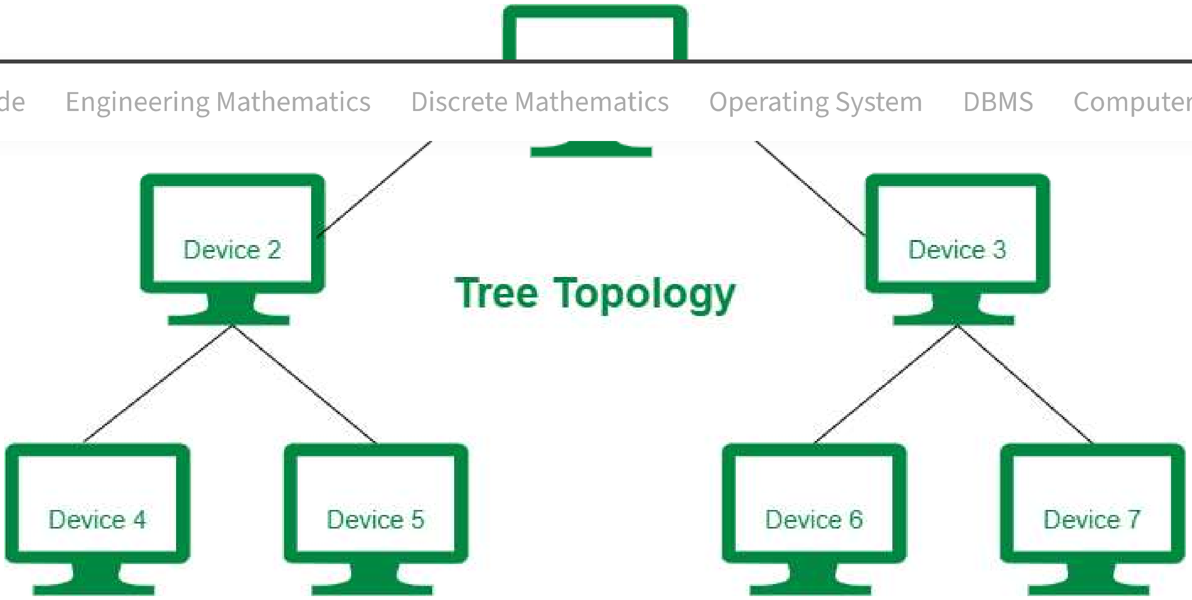
Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

Tree Topology

Tree topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and **SAC (Standard Automatic Configuration)** are used.

Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw



Tree Topology

In tree topology, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e.

from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add **new devices to the existing network.**
- **Error detection** and **error correction** are very easy in a tree topology.

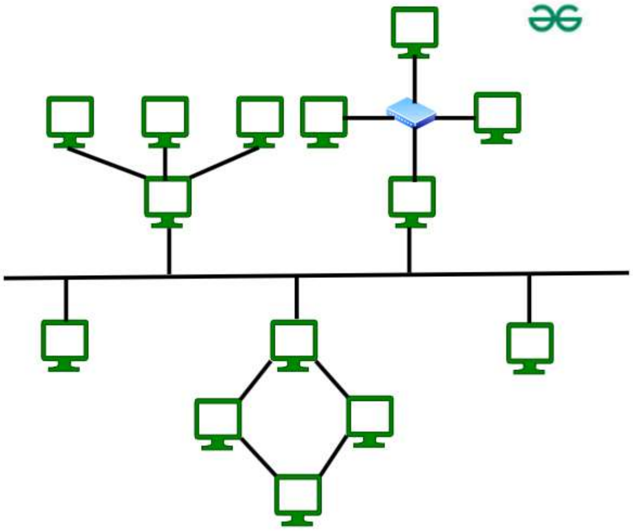
Disadvantages of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

Hybrid Topology

Hybrid Topology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Hybrid Topology

The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

Advantages of Hybrid Topology

- This topology is **very flexible** .
- The size of the network can be easily expanded by **adding new devices.**

Disadvantages of Hybrid Topology

- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**
- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices** .

A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

Why is Network Topology Important?

Network Topology is important because it defines how devices are connected and how they communicate in the network. Here are some points that defines why network topology is important.

- **Network Performance:** Upon choosing the appropriate topology as per requirement, it helps in running the network easily and hence increases network performance.
- **Network Reliability:** Some topologies like Star, Mesh are reliable as if one connection fails, they provide an alternative for that connection, hence it works as a backup.
- **Network Expansion** : Chosing correct topology helps in easier expansion of Network as it helps in adding more devices to the network without disrupting the actual network.
- **Network Security:** Network Topology helps in understanding how devices are connected and hence provides a better security to the network.

Conclusion

In conclusion, network topologies play a crucial role in determining the efficiency and reliability of a computer network. Each topology, whether it's bus, star, ring, mesh, or tree, offers unique benefits and potential drawbacks. By understanding these different arrangements, network designers can choose the most appropriate topology to meet the specific needs of their systems, ensuring optimal performance and connectivity.

Comment More info Advertise with us

Next Article

Difference between Physical and Logical Topology

Introduction to basic Networking Terminology

Last Updated : 13 Mar, 2023

For a specific purpose if things are connected together, are referred to as a **NETWORK**. A network can be of many types, like a telephone network, television network, computer network, or even a people network.

Similarly, a **COMPUTER NETWORK** is also a kind of setup, where it connects two or more devices to share a range of services and information in the form of **e-mails and messages**, **databases**, **documents**, **websites**, **audios and videos**, **telephone calls**, **and video conferences**, etc. among them.

A **PROTOCOL** is nothing but a set of defined **rules**, which has to be followed by every connected device across a network to communicate and share information among them. To facilitates **End to End** communication, a number of protocols worked together to form **Protocol Suites or Stacks**.

Networking terminology can be confusing, especially for those who are new to computer networking. Here are some basic terms and their definitions to help you understand the fundamentals of networking:

Network: A collection of interconnected devices, such as computers, printers, and servers, that can communicate with each other.

Node: Any device connected to a network, such as a computer, printer, or router.

Protocol: A set of rules and standards that define how devices on a network communicate with each other.

IP Address: A unique numerical identifier assigned to each device on a network, used to identify and communicate with other devices.

Router: A networking device that connects multiple networks together and forwards data packets between them.

Switch: A networking device that connects devices on a network and forwards data packets between them.

Firewall: A security device or software that monitors and controls incoming and outgoing network traffic, based on a set of predefined security rules.

DNS (Domain Name System): A system that translates domain names (such as www.example.com) into IP addresses, allowing devices to locate and connect to websites and other network resources.

LAN (Local Area Network): A network that connects devices within a limited geographical area, such as a home, office, or building.

WAN (Wide Area Network): A network that connects devices over a large geographical area, such as multiple offices in different cities or

DHCP (Dynamic Host Configuration Protocol): A protocol that automatically assigns IP addresses and network configuration settings to devices on a network.

TCP/IP (Transmission Control Protocol/Internet Protocol): A set of protocols used to communicate over the internet and other networks.

These are just a few basic networking terms, but understanding them is essential to building a strong foundation in computer networking.

Some basic Protocols are:

- **IP** : Internet Protocol

- **FTP** : File Transfer Protocol
- **SMTP** : Simple Mail Transfer Protocol
- **HTTP** : Hyper Text Transfer Protocol

The **Network reference models** were developed to allow products from different manufacturers to interoperate on a network. A network reference model serves as a blueprint, detailing standards for how protocol communication should occur.

The most widely recognized reference models are the **Open Systems Interconnect** (**OSI**) Model and **Department of Defense** (DoD, also known as **TCP/IP**) model.

- **LANs (Local Area Networks)**
- **MANs (Metropolitan Area Networks)**
- **WANs (Wide Area Networks)**

An **Internetwork** is a general term describing multiple networks connected together. The Internet is the largest and most well-known internetwork.

- **SAN (Storage Area Network)**: A SAN provides systems with high-speed, lossless access to high-capacity storage devices.
- **VPN (Virtual Private Network)**: A VPN allows for information to be securely sent across a public or unsecured network, such as the Internet. Common uses of a VPN are to connect branch offices or remote users to the main office.

- A host can act as a ***Client*** when he is requesting information.
- A host can act as a ***Server*** when he provides information.
- A host can also request and provide information, which is called ***Peer***.

Types of area networks - LAN, MAN and WAN

Last Updated : 27 Dec, 2024

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN, and WAN are the three major types of networks designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area, **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.

There are other types of Computer Networks also, like :

- PAN (Personal Area Network)
- SAN (Storage Area Network)
- EPN (Enterprise Private Network)
- VPN (Virtual Private Network)

Personal Area Network (PAN)-

PAN is a personal area network having an interconnection of personal technology devices to communicate over a short distance. It covers only less than 10 meters or 33 feet of area. PAN has fewer users as compared to other networks such as LAN, WAN, etc. PAN typically uses some form of wireless technology. PAN involves the transmission of data between information devices such as smartphones, personal computers, tablet computers, etc.

Advantages:

- Allows for easy communication between personal devices in close proximity.
- Can be set up easily and quickly.

- Uses wireless technology, which eliminates the need for wires and cables.
- PANs are designed to be energy efficient, which means that devices can communicate with each other without draining their batteries quickly.
- PANs are typically secured using encryption and authentication protocols, which helps to prevent unauthorized access to data and resources.

Disadvantages:

- Limited coverage area.
- May not be suitable for large-scale data transfer or communication.PANs typically have limited bandwidth, which means that they may not be able to handle large amounts of data or high-speed communication.
- May experience interference from other wireless devices.

Local Area Network (LAN) –

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked is limited. By definition, the connections must be high-speed and relatively inexpensive hardware (Such as hubs, network adapters, and Ethernet cables). LANs cover a smaller geographical area (Size is limited to a few kilometres) and are privately owned. One can use it for an office building, home, hospital, school, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. LAN has a range up to 2km. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example A bunch of students playing Counter-Strike in the same room (without internet).

Advantages:

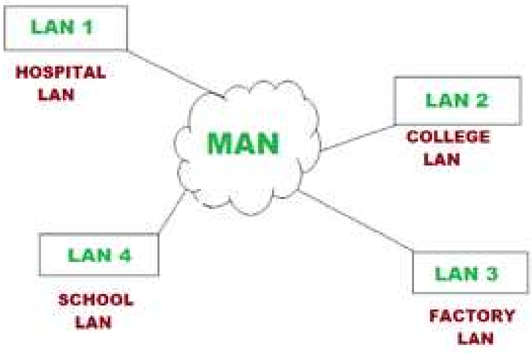
- Provides fast data transfer rates and high-speed communication.
- Easy to set up and manage.
- Can be used to share peripheral devices such as printers and scanners.
- Provides increased security and fault tolerance compared to WANs.

Disadvantages:

- Limited geographical coverage.
- Limited scalability and may require significant infrastructure upgrades to accommodate growth.
- May experience congestion and network performance issues with increased usage.

Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that covered by a LAN and a smaller area as compared to WAN. MAN has a range of 5-50km. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It’s hard to design and maintain a Metropolitan Area Network.



The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN are moderate. Devices used for transmission of data through MAN are Modem and Wire/Cable. Examples of a MAN are part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

Advantages:

- Provides high-speed connectivity over a larger geographical area than LAN.
- Can be used as an ISP for multiple customers.
- Offers higher data transfer rates than WAN in some cases.

Disadvantages:

- Can be expensive to set up and maintain.
- May experience congestion and network performance issues with increased usage.
- May have limited fault tolerance and security compared to LANs.

Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. WAN has a range of above 50 km. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high-speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN(Public Switched Telephone Network) or Satellite Link. Due to long-distance transmission, the noise and error tend to be more in WAN.

WAN's data rate is slow about a 10th LAN's speed since it involves increased distance and increased number of servers and terminals etc. The speed of WAN ranges from a few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for the transmission of data through WAN are Optic wires, Microwaves, and Satellites. An example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is a dial-up line that connects a home computer to the Internet.

Advantages:

- Covers large geographical areas and can connect remote locations.
- Provides connectivity to the internet.
- Offers remote access to resources and applications.
- Can be used to support multiple users and applications simultaneously.

Disadvantages:

- Can be expensive to set up and maintain.
- Offers slower data transfer rates than LAN or MAN.
- May experience higher latency and longer propagation delays due to longer distances and multiple network hops.
- May have lower fault tolerance and security compared to LANs.

Conclusion –

There are many advantages of LAN over MAN and WAN, such as LAN provide excellent reliability, a high data transmission rate, and can easily be managed and shares peripheral devices too. Local Area Network cannot cover cities or towns and for that Metropolitan Area

Network is needed, which can connect a city or a group of cities together. Further, for connecting a Country or a group of Countries one requires a Wide Area Network.

Comment More info Advertise with us

Next Article

Introduction to Internet

Similar Reads

1. Types and Uses of Backbone Networks
2. Types of MANET in Computer Network
3. Overview of Campus Area Network (CAN)
4. Advantages and Disadvantages of Personal Area Network
5. Types of Broadcast Network
6. Areas of Network Management
7. Types of Internetwork
8. Types of Computer Networks
9. Types of Computer Networks
10. What is LAN (Local Area Network)? Understanding LAN's Working, Types and Features

---

Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Registered Address:
K 061, Tower K, Gulshan Vivante
Apartment, Sector 137, Noida, Gautam
Buddh Nagar, Uttar Pradesh, 201305

TCP/IP Model

Last Updated : 08 May, 2025

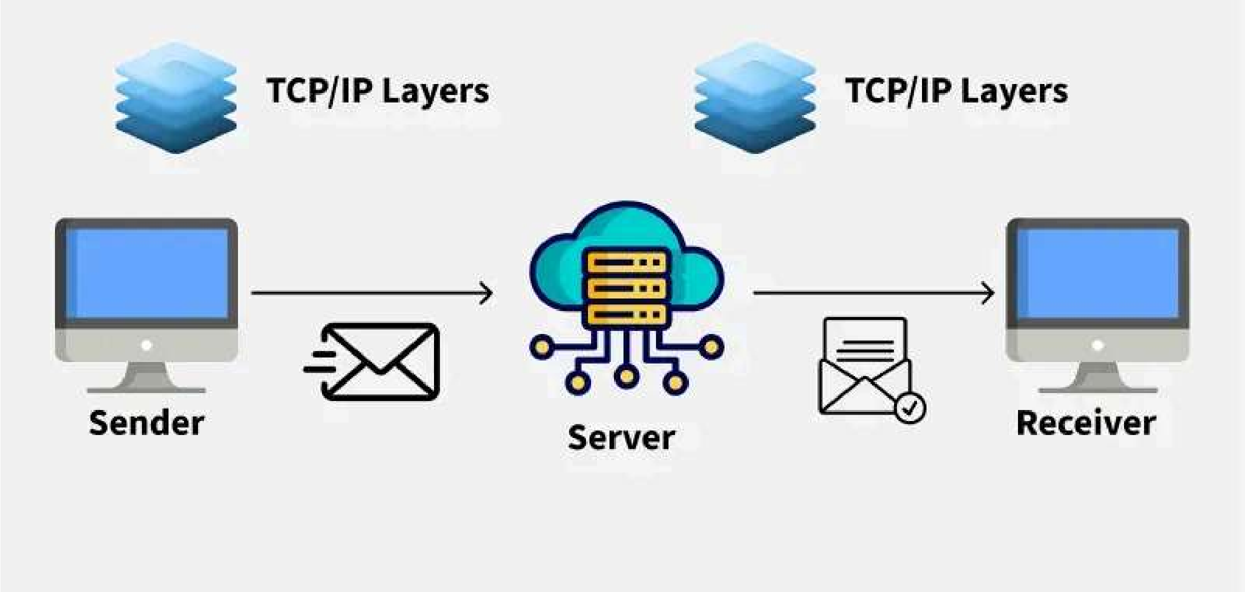
The TCP/IP model (Transmission Control Protocol/Internet Protocol) is a four-layer networking framework that enables reliable communication between devices over interconnected networks. It provides a standardized set of protocols for transmitting data across interconnected networks, ensuring efficient and error-free delivery. Each layer has specific functions that help manage different aspects of network communication, making it essential for understanding and working with modern networks.

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1970s and is based on standard protocols. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

Role of TCP/IP

TCP/IP enables interoperability between diverse systems over various network types (e.g., copper, fiber, wireless). It ensures seamless communication across LANs, WANs, and the internet. Without TCP/IP, large-scale global networking would not be possible.

The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.


TCP/IP Layers
TCP/IP Layers
Sender
Server
Receiver

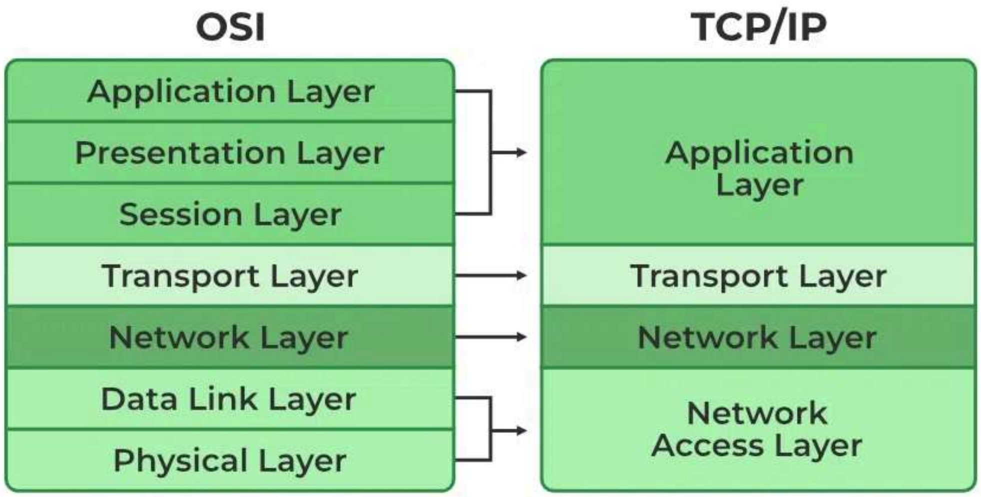
TCP

Layers of TCP/IP Model

It's composed of four interconnected layers compared to the seven layers in the OSI model. Each layer performs a specific task on the data that is being transmitted over the network channel, and data moves from one layer to another.

- Application Layer
- Transport Layer(TCP/UDP)
- Network/Internet Layer(IP)
- Network Access Layer

The diagrammatic comparison of the **TCP/IP and OSI** model is as follows:


OSI
TCP/IP
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Network Layer
Network Access Layer

TCP/IP and OSI MODEL

1. Application Layer

The Application Layer is the closest to the end user and is where applications and user interfaces reside. It serves as the bridge between user programs and the lower layers responsible for data transmission.

- **Function:** Provides services and interfaces for end-user applications to access network resources.
- **Key responsibilities:**
    - Supports application protocols like HTTP, FTP, SMTP, DNS, etc.
    - Enables communication between software applications across networks.
    - Handles data formatting, encryption, and session management.

2. Transport Layer

This layer ensures data is delivered reliably and in the correct order between devices. The two main protocols in this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

- **Function:** Ensures reliable or unreliable delivery of data between hosts.
- **Key responsibilities:**
    - TCP (Transmission Control Protocol): Provides reliable, connection-oriented delivery with error checking, retransmission, and flow control.
    - UDP (User Datagram Protocol): Provides faster, connectionless transmission without guarantees.
    - Manages flow control and segmentation/reassembly of data.

3. Internet Layer

It handles the routing of data packets across networks. It uses the Internet Protocol (IP) to assign unique IP addresses to devices and decide the most efficient path for data to reach its destination.

- **Function:** Determines the best path for data to travel across networks.
- **Key responsibilities:**
    - IP (Internet Protocol)**:** Provides addressing and routing.
    - Handles packet forwarding, fragmentation, and logical addressing (IP addresses).
    - Involves protocols like IP, ICMP (for diagnostics), and ARP (for address resolution).

4. Network Access Layer

This layer is the lowest layer in the model and responsible for the physical connection between devices within the same network segment.

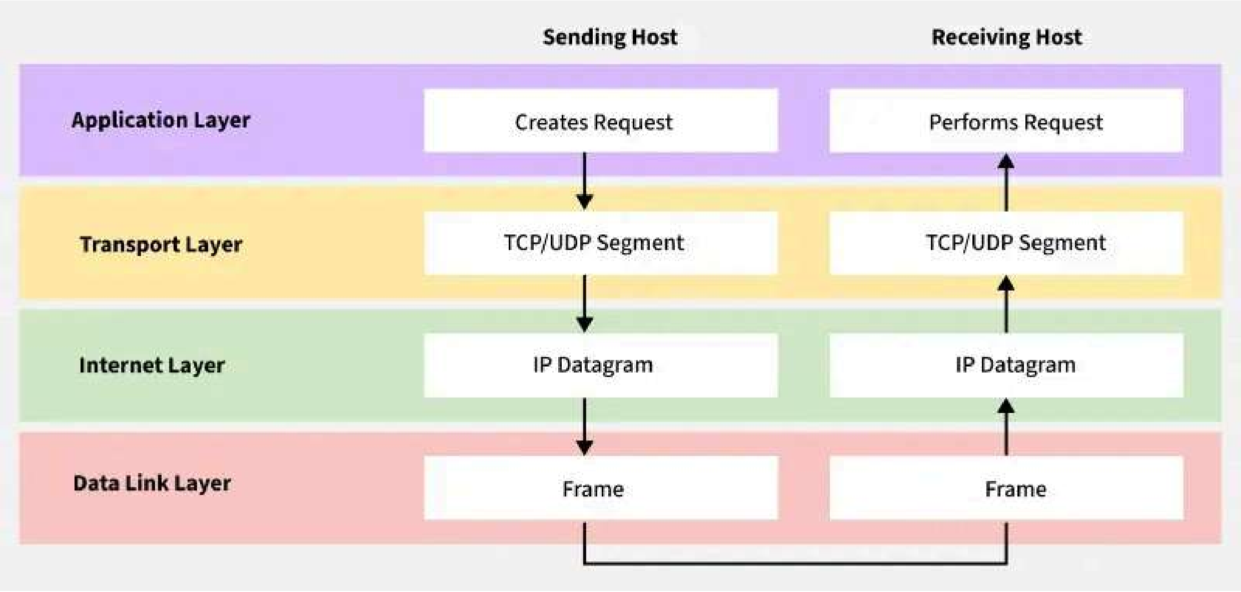
- **Function:** Manages the physical transmission of data over the network hardware.
- **Key responsibilities:**
    - Handles how data is physically sent over cables, Wi-Fi, etc.
    - Manages MAC addressing, framing, and error detection at the physical link.
    - Includes Ethernet, Wi-Fi, and other data link technologies.

Working of TCP/IP Model

When Sending Data (From Sender to Receiver)

- **Application Layer**
    - A user sends data through an application (e.g., opening a website via a browser).
    - The application prepares data for transmission (e.g., using **HTTP**, **FTP**, **SMTP**).

- **Transport Layer (TCP/UDP)**
    - TCP breaks data into small segments, adds a header (with sequence numbers, source/destination ports).
    - Ensures reliable delivery (TCP) or fast, connectionless delivery (UDP).
- **Internet Layer (IP)**
    - Adds IP addresses to each packet (source and destination).
    - Determines the route the packet should take to reach the destination.
- **Link Layer (Network Access Layer)**
    - Converts packets into frames, adds MAC (physical) addresses.
    - Sends data as binary bits (0s and 1s) over the physical medium (e.g., Ethernet, Wi-Fi).


Sending Host
Receiving Host
Application Layer
Creates Request
Performs Request
Transport Layer
TCP/UDP Segment
TCP/UDP Segment
Internet Layer
IP Datagram
IP Datagram
Data Link Layer
Frame
Frame

TCP/IP WORKING MODEL

When Receiving Data (At the Destination)

Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw

- **Link Layer**
    - Receives bits and reconstructs frames.
    - Passes frames up to the Internet layer.
- **Internet Layer**

  - Reads the IP address to confirm it's the correct recipient.
  - Removes the IP header and sends the data to the Transport layer.
- **Transport Layer**
  - Reassembles TCP segments in the correct order.
  - Verifies data integrity using acknowledgments and checksums.
- **Application Layer**
  - The data is delivered to the appropriate application (e.g., browser displays a web page).

Why TCP/IP is Used Over the OSI Model

Reason	Explanation
Simpler Structure	TCP/IP has only 4 layers, compared to 7 in OSI, making it easier to implement and understand in real systems.
Protocol-Driven Design	TCP/IP was designed based on working protocols, while the OSI model is more of a theoretical framework.
Flexibility and Robustness	TCP/IP adapts well to different hardware and networks and includes error handling, routing, and congestion control.
Open Standard	TCP/IP is open, free to use, and not controlled by any single organization, helping it gain universal acceptance.
Actual Use vs Conceptual Model	The OSI model is great for education and design principles, but TCP/IP is the one actually used in real-world networking.

Advantages of TCP/IP Model

- **Interoperability** : The TCP/IP model allows different types of computers and networks to communicate with each other, promoting compatibility and cooperation among diverse systems.

- **Scalability** : TCP/IP is highly scalable, making it suitable for both small and large networks, from local area networks (LANs) to wide area networks (WANs) like the internet.

- **Standardization** : It is based on open standards and protocols, ensuring that different devices and software can work together without compatibility issues.

- **Flexibility** : The model supports various routing protocols, data types, and communication methods, making it adaptable to different networking needs.

- **Reliability** : TCP/IP includes error-checking and retransmission features that ensure reliable data transfer, even over long distances and through various network conditions.

Disadvantages of TCP/IP Model

- **Security Concerns** : TCP/IP was not originally designed with security in mind. While there are now many security protocols available (such as SSL/TLS), they have been added on top of the basic TCP/IP model, which can lead to vulnerabilities.

- **Inefficiency for Small Networks** : For very small networks, the overhead and complexity of the TCP/IP model may be unnecessary and inefficient compared to simpler networking protocols.

- **Limited by Address Space** : Although IPv6 addresses this issue, the older IPv4 system has a limited address space, which can lead to issues with address exhaustion in larger networks.

- **Data Overhead** : TCP the transport protocol, includes a significant amount of overhead to ensure reliable transmission. This can reduce efficiency, especially for small data packets or in networks where speed is crucial.

Comment More info Advertise with us

Next Article

TCP/IP Ports and Its Applications

Similar Reads

1. OSI, TCP/IP and Hybrid Models
2. History of TCP/IP
3. Computer Network Models
4. TCP/IP Packet Format
5. Transport Layer in OSI Model
6. Adhoc TCP
7. TCP Congestion Control
8. Network Layer in OSI Model
9. Devices used in each layer of TCP/IP model
10. Types of Socket

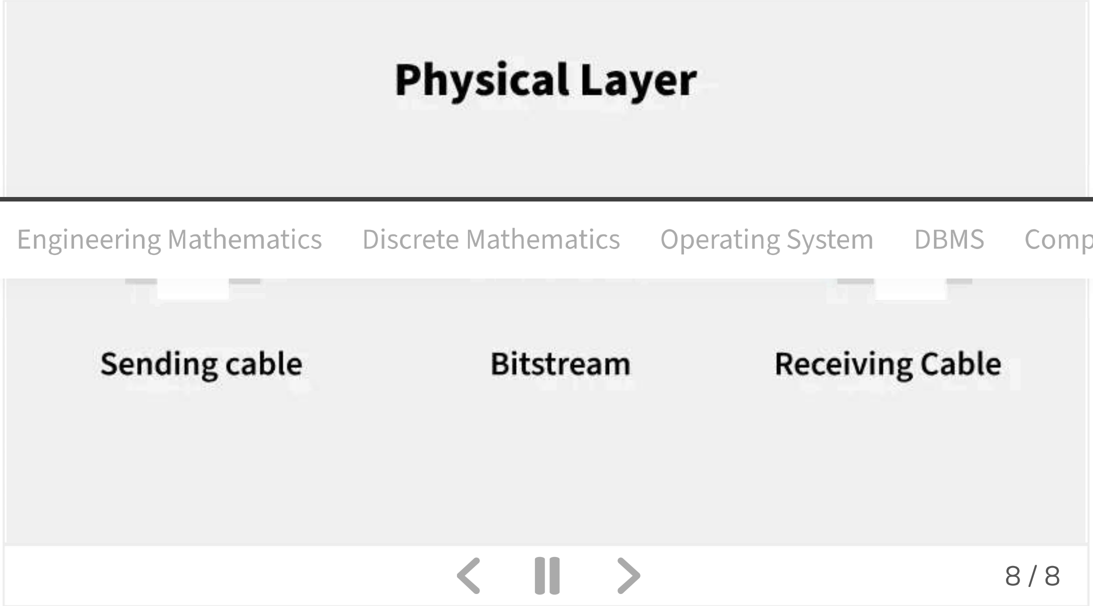
Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Registered Address:
K 061, Tower K, Gulshan Vivante
Apartment, Sector 137, Noida, Gautam
Buddh Nagar, Uttar Pradesh, 201305

What is OSI Model? - Layers of OSI Model

Last Updated : 22 May, 2025

The **OSI (Open Systems Interconnection)** Model is a set of rules that explains how different computer systems communicate over a network. OSI Model was developed by the **International Organization for Standardization (ISO)**. The OSI Model consists of 7 layers and each layer has specific functions and responsibilities. This layered approach makes it easier for different devices and technologies to work together. OSI Model provides a clear structure for data transmission and managing network issues. The OSI Model is widely used as a reference to understand how network systems function.



Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw

Layers of the OSI Model

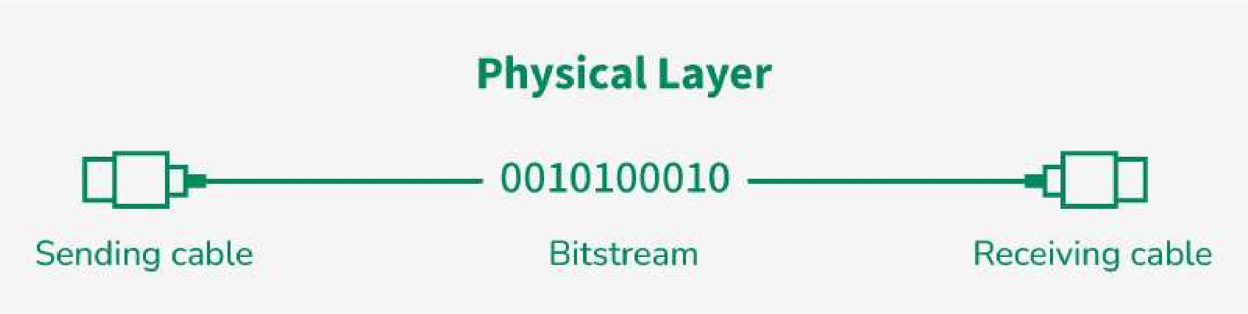
There are 7 layers in the OSI Model and each layer has its specific role in handling data. All the layers are mentioned below:

- Physical Layer
- Data Link Layer

- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Layer 1: Physical Layer

The lowest layer of the OSI reference model is the **Physical Layer**. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** Physical Layer is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together. Common physical layer devices are Hub, Repeater, Modem, and Cables.



Physical Layer

Functions of the Physical Layer

- **Bit Synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit Rate Control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical Topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus topology, star topology, or mesh topology.

- **Transmission Mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full duplex.

Layer 2: Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address. Packet in the Data Link layer is referred to as Frame**.** Switches and Bridges are common Data Link Layer devices.

The Data Link Layer is divided into two sublayers:

- Logical Link Control (LLC)
- Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of the **NIC (Network Interface Card)**. DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking, "Who has that IP address?" and the destination host will reply with its MAC address.

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical Addressing:** After creating frames, the Data link layer adds physical addresses (MAC **addresses)** of the sender and/or receiver in the header of each frame.

- **Error Control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- **Access Control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Layer 3: Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender and receiver's IP address are placed in the header by the network layer. Segment in the Network layer is referred to as Packet**.** Network layer is implemented by networking devices such as routers and switches.

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender and receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Layer 4: Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as **Segments**. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found. Protocols used in Transport Layer are TCP, UDP NetBIOS, PPTP.

At the sender's side, the transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow and error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

- Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

At the Receiver's side, Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus, by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

- Connection-Oriented Service

- Connectionless Service

Layer 5: Session Layer

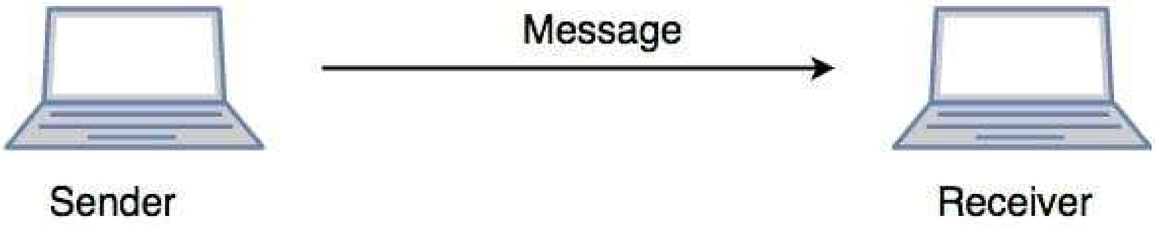
Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP.

Functions of the Session Layer

- **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely, and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full duplex.

Example

Let us consider a scenario where a user wants to send a message through some Messenger application running in their browser. The "**Messenger**" here acts as the application layer which provides the user with an interface to create the data. This message or so-called **Data** is compressed, optionally encrypted (if the data is sensitive), and converted into bits (0's and 1's) so that it can be transmitted.



Communication in Session Layer

Layer 6: Presentation Layer

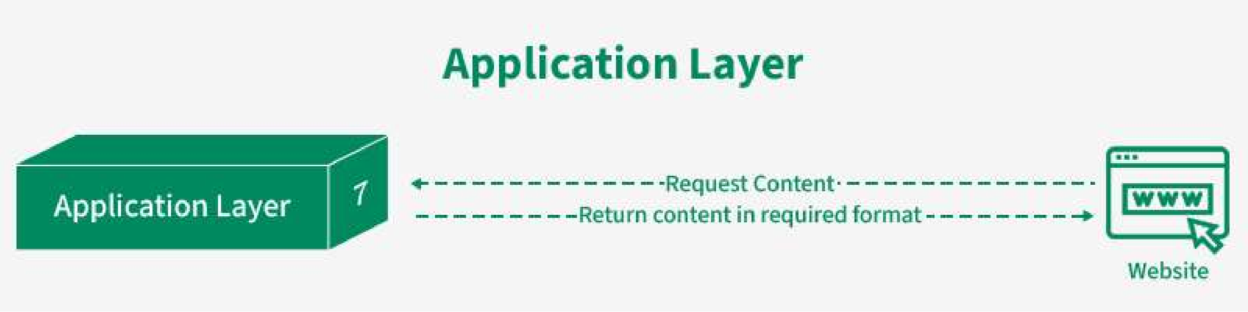
The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. Protocols used in the Presentation Layer are TLS/SSL (Transport Layer Security / Secure Sockets Layer).JPEG, MPEG, GIF, are standards or formats used for encoding data, which is part of the presentation layer's role.

Functions of the Presentation Layer

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext, and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

Layer 7: Application Layer

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. Protocols used in the Application layer are SMTP, FTP, DNS, etc.



Application Layer

Functions of the Application Layer

The main functions of the application layer are given below.

- **Network Virtual Terminal (NVT):** It allows a user to log on to a remote host.
- **File Transfer Access and Management (FTAM):** This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.
- **Mail Services:** Provide email service.
- **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

How Data Flows in the OSI Model?

When we transfer information from one device to another, it travels through 7 layers of OSI model. First data travels down through 7 layers from the sender's end and then climbs back 7 layers on the receiver's end.

Data flows through the OSI model in a step-by-step process:

- **Application Layer:** Applications create the data.
- **Presentation Layer:** Data is formatted and encrypted.
- **Session Layer:** Connections are established and managed.
- **Transport Layer:** Data is broken into segments for reliable delivery.
- **Network Layer:** Segments are packaged into packets and routed.
- **Data Link Layer:** Packets are framed and sent to the next device.
- **Physical Layer:** Frames are converted into bits and transmitted physically.

Each layer adds specific information to ensure the data reaches its destination correctly, and these steps are reversed upon arrival.

PH: Presentation Header
Data
Device A
Device B
07 Application Layer
Data
1 / 8

We can understand how data flows through OSI Model with the help of an example mentioned below.

Let us suppose, **Person A** sends an e-mail to his friend **Person B**.

Step 1: Person A interacts with e-mail application like **Gmail**, **outlook**, etc. Writes his email to send. (This happens at **Application Layer**).

Step 2: At Presentation Layer, Mail application prepares for data transmission like encrypting data and formatting it for transmission.

Step 3: At Session Layer, there is a connection established between the sender and receiver on the internet.

Step 4: At Transport Layer, Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information.

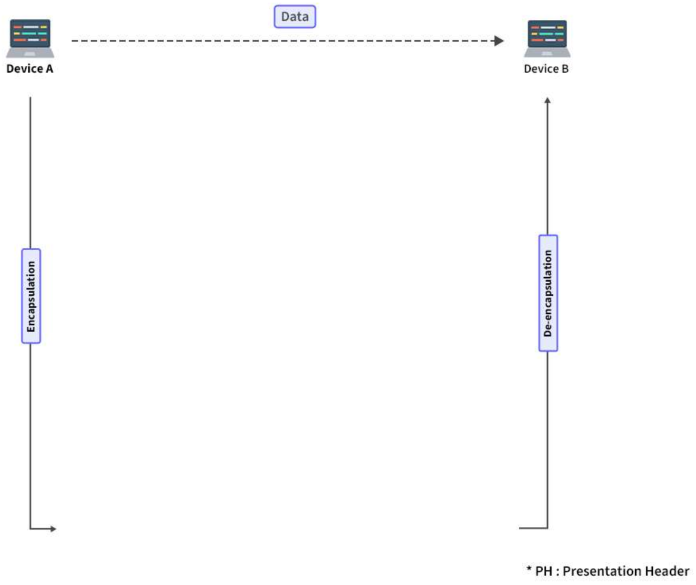
Step 5: At Network Layer, addressing of packets is done in order to find the best route for transfer.

Step 6: At Data Link Layer, data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection.

Step 7: At Physical Layer, Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.

After the email reaches the receiver i.e. **Person B**, the process will reverse and decrypt the e-mail content. At last, the email will be shown on **Person B** email client.

Please refer the below animation for detailed flow.


Data
Device A
Device B
Encapsulation
De-encapsulation
* PH : Presentation Header

Protocols Used in the OSI Layers

Layer	Working	Protocol Data Unit	Protocols
1: Physical Layer	Establishing Physical Connections between Devices.	Bits	USB, SONET/SDH, etc.
2: Data Link Layer	Node to Node Delivery of Message.	Frames	Ethernet, PPP, etc.
3: Network Layer	Transmission of data from one host to another, located in different networks.	Packets	IP, ICMP, IGMP, OSPF, etc.
4: Transport Layer	Take Service from Network Layer and	Segments (for TCP) or	TCP, UDP, SCTP, etc.

Layer	Working	Protocol Data Unit	Protocols
	provide it to the Application Layer.	Datagrams (for UDP)	
5: Session Layer	Establishes Connection, Maintenance, Ensures Authentication and Ensures security.	Data	NetBIOS, RPC, PPTP, etc.
6: Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Data	TLS/SSL, MIME, etc.
7: Application Layer	Helps in identifying the client and synchronizing communication.	Data	FTP, SMTP, DNS, DHCP, etc.

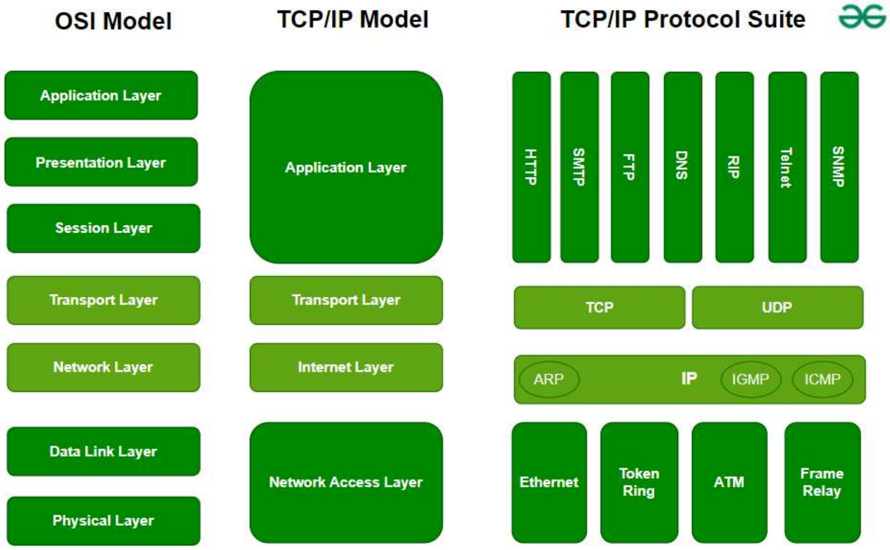
Why Does the OSI Model Matter

The OSI Model matters because it provides the user a clear structure of "how the data moves in the network?". As the OSI Model consists of 7 layers, each layer has its specific role, and due to which it helps in understanding, identifying and solving the complex network problems easily by focusing on one of the layers not the entire network.

As the modern Internet does not prefer the OSI Model, but still, the OSI Model is still very helpful for solving network problems. It helps people understanding network concepts very easily.

Difference Between OSI and TCP/IP Model

OSI Model	TCP/IP Model
OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
OSI model has 7 layers.	TCP/IP model consists of 4 layers.
Package delivery is guaranteed in OSI Model.	Package delivery is not guaranteed in the TCP/IP Model.
In the OSI model, only layers 1,2 and 3 are necessary for data transmission.	All layers of the TCP/IP model are needed for data transmission.
Protocols at each layer is independent of the other layer.	Layers are integrated; some layers are required by other layers of TCP/IP model.
OSI Model is a conceptual framework, less used in practical applications.	Widely used in actual networks like Internet and Communication Systems.


OSI Model
TCP/IP Model
TCP/IP Protocol Suite
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Internet Layer
Network Access Layer
HTTP
SMTP
FTP
DNS
RIP
Telnet
SNMP
TCP
UDP
ARP
IP
IGMP
ICMP
Ethernet
Token Ring
ATM
Frame Relay

OSI vs TCP/IP

Advantages of OSI Model

The OSI Model defines the communication of a computing system into 7 different layers. Its advantages include:

- It divides network communication into 7 layers which makes it easier to understand and troubleshoot.
- It standardizes network communications, as each layer has fixed functions and protocols.
- Diagnosing network problems is easier with the **OSI model.**
- It is easier to improve with advancements as each layer can get updates separately.

Disadvantages of OSI Model

- The OSI Model has seven layers, which can be complicated and hard to understand for beginners.
- In real-life networking, most systems use a simpler model called the Internet protocol suite (TCP/IP), so the OSI Model is not always directly applicable.
- Each layer in the OSI Model adds its own set of rules and operations, which can make the process more time-consuming and less efficient.
- The OSI Model is more of a theoretical framework, meaning it's great for understanding concepts but not always practical for implementation.

Comment More info Advertise with us

Next Article

Physical Layer in OSI Model

Similar Reads

1. Physical Layer in OSI Model
2. Functions of Physical layer in OSI Model
3. Network Layer in OSI Model
4. Session Layer in OSI model

What is Ethernet?

Last Updated : 28 Nov, 2024

A LAN is a data communication network connecting various terminals or computers within a building or limited geographical area. The connection between the devices could be wired or wireless. Ethernet, Token rings, and Wireless LAN using IEEE 802.11 are examples of standard LAN technologies.In this article we will see ethernet in detail.

Ethernet

IEEE standards 802.3. The reason behind its wide usability is that Ethernet is easy to understand, implement, and maintain, and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of the topologies that are allowed. Ethernet generally uses a bus topology. Ethernet operates in two layers of the OSI model, the physical layer and the data link layer. For Ethernet, the protocol data unit is a frame since we mainly deal with DLLs. In order to handle collisions, the Access control mechanism used in Ethernet is CSMA/CD.

Although Ethernet has been largely replaced by wireless networks.A wired networking still uses Ethernet more frequently. Wi-Fi eliminates the need for cables by enabling users to connect their smartphones or laptops to a network wirelessly. The 802.11ac Wi-Fi standard offers faster maximum data transfer rates when compared to Gigabit Ethernet. However, wired connections are more secure and less susceptible to interference than wireless networks.

History of Ethernet

Robert Metcalfe's invention of Ethernet in 1973 completely changed computer networking. With Ethernet Version 2's support for 10 Mbps and an initial data rate of 2.94 Mbps, it first gained popularity in 1982. Ethernet's adoption was accelerated by the IEEE 802.3 standardization in 1983. Local area networks (LANs) and the internet were able to expand quickly because of the rapid evolution and advancement of Ethernet, which over time reached speeds of 100 Mbps, 1 Gbps, 10 Gbps, and higher. It evolved into the standard technology for wired network connections, enabling dependable and quick data transmission for private residences, commercial buildings, and data centers all over the world.

There are different types of Ethernet networks that are used to connect devices and transfer data.

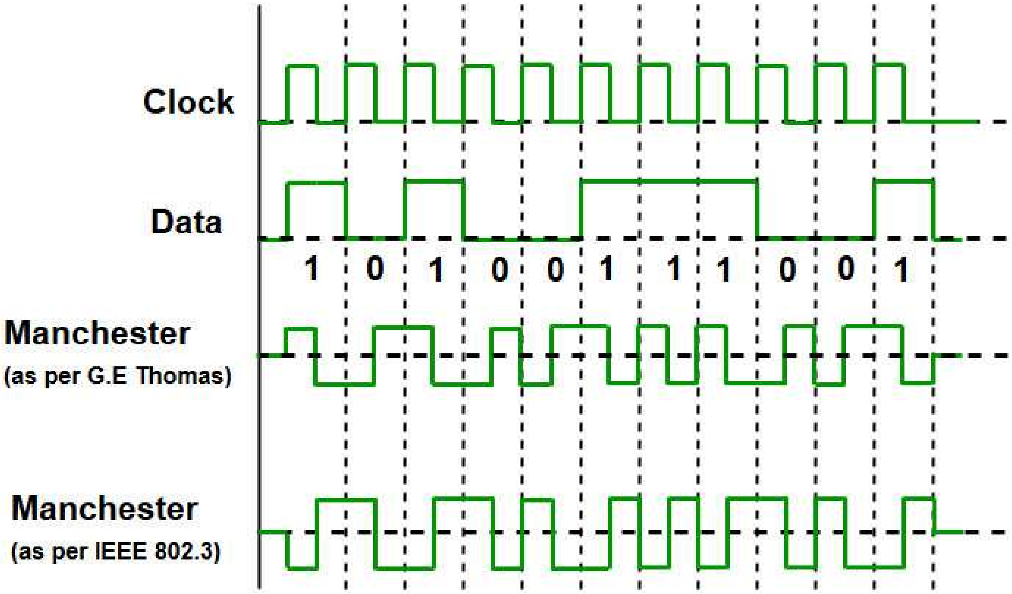
Let's discuss them in simple terms:

1. **Fast Ethernet:** This type of Ethernet network uses cables called twisted pair or CAT5. It can transfer data at a speed of around 100 Mbps (megabits per second). Fast Ethernet uses both fiber optic and twisted pair cables to enable communication. There are three categories of Fast Ethernet: 100BASE-TX, 100BASE-FX, and 100BASE-T4.
2. **Gigabit Ethernet:** This is an upgrade from Fast Ethernet and is more common nowadays. It can transfer data at a speed of 1000 Mbps or 1 Gbps (gigabit per second). Gigabit Ethernet also uses fiber optic and twisted pair cables for communication. It often uses advanced cables like CAT5e, which can transfer data at a speed of 10 Gbps.
3. **10-Gigabit Ethernet:** This is an advanced and high-speed network that can transmit data at a speed of 10 gigabits per second. It uses special cables like CAT6a or CAT7 twisted-pair cables and fiber optic cables. With the help of fiber optic cables, this network can cover longer distances, up to around 10,000 meters.
4. **Switch Ethernet:** This type of network involves using switches or hubs to improve network performance. Each workstation in this network has its own dedicated connection, which improves the speed and efficiency

of data transfer. Switch Ethernet supports a wide range of speeds, from 10 Mbps to 10 Gbps, depending on the version of Ethernet being used.

In summary, Fast Ethernet is the basic version with a speed of 100 Mbps, Gigabit Ethernet is faster with a speed of 1 Gbps, 10-Gigabit Ethernet is even faster with a speed of 10 Gbps, and Switch Ethernet uses switches or hubs to enhance network performance.The Manchester Encoding Technique is used in Ethernet. Using Manchester encoding, data can be transmitted over a physical medium in communication systems. It is a type of line coding where the signal transitions, as opposed to the absolute voltage levels, serve as the data representation.

Each bit of information is split into two equal time periods, or "halves," in Manchester encoding. If the signal level is higher during the first half of the bit period than it is during the second, the result is a logic high (typically 1), or vice versa.



Since we are talking about IEEE 802.3 standard Ethernet, therefore, 0 is expressed by a high-to-low transition, a 1 by the low-to-high transition. In both Manchester Encoding and Differential Manchester, the Encoding Baud rate is double of bit rate.

Key Features of Ethernet

1. **Speed:** Ethernet is capable of transmitting data at high speeds, with current Ethernet standards supporting speeds of up to 100 Gbps.
2. **Flexibility:** Ethernet is a flexible technology that can be used with a wide range of devices and operating systems. It can also be easily scaled to accommodate a growing number of users and devices.
3. **Reliability:** Ethernet is a reliable technology that uses error-correction techniques to ensure that data is transmitted accurately and efficiently.
4. **Cost-effectiveness:** Ethernet is a cost-effective technology that is widely available and easy to implement. It is also relatively low-maintenance, requiring minimal ongoing support.
5. **Interoperability:** Ethernet is an interoperable technology that allows devices from different manufacturers to communicate with each other seamlessly.
6. **Security:** Ethernet includes built-in security features, including encryption and authentication, to protect data from unauthorized access.
7. **Manageability:** Ethernet networks are easily managed, with various tools available to help network administrators monitor and control network traffic.
8. **Compatibility:** Ethernet is compatible with a wide range of other networking technologies, making it easy to integrate with other systems and devices.
9. **Availability:** Ethernet is a widely available technology that can be used in almost any setting, from homes and small offices to large data centers and enterprise-level networks.
10. **Simplicity:** Ethernet is a simple technology that is easy to understand and use. It does not require specialized knowledge or expertise to set up and configure, making it accessible to a wide range of users.
11. **Standardization:** Ethernet is a standardized technology, which means that all Ethernet devices and systems are designed to work together seamlessly. This makes it easier for network administrators to manage and troubleshoot Ethernet networks.

12. **Scalability:** Ethernet is highly scalable, which means it can easily accommodate the addition of new devices, users, and applications without sacrificing performance or reliability.
13. **Broad compatibility:** Ethernet is compatible with a wide range of protocols and technologies, including TCP/IP, HTTP, FTP, and others. This makes it a versatile technology that can be used in a variety of settings and applications.
14. **Ease of integration:** Ethernet can be easily integrated with other networking technologies, such as Wi-Fi and Bluetooth, to create a seamless and integrated network environment.
15. **Ease of troubleshooting:** Ethernet networks are easy to troubleshoot and diagnose, thanks to a range of built-in diagnostic and monitoring tools. This makes it easier for network administrators to identify and resolve issues quickly and efficiently.
16. **Support for multimedia:** Ethernet supports multimedia applications, such as video and audio streaming, making it ideal for use in settings where multimedia content is a key part of the user experience.Ethernet is a reliable, cost-effective, and widely used LAN technology that offers high-speed connectivity and easy manageability for local networks.

Advantages of Ethernet

Speed: When compared to a wireless connection, Ethernet provides significantly more speed. Because Ethernet is a one-to-one connection, this is the case. As a result, speeds of up to 10 Gigabits per second (Gbps) or even 100 Gigabits per second (Gbps) are possible.

Efficiency: An Ethernet cable, such as Cat6, consumes less electricity, even less than a wifi connection. As a result, these ethernet cables are thought to be the most energy-efficient.

Good data transfer quality: Because it is resistant to noise, the information transferred is of high quality.

```
Baud rate = 2* Bit rate
```

Disadvantages of Ethernet

Distance limitations: Ethernet has distance limitations, with the maximum cable length for a standard Ethernet network being 100 meters. This means that it may not be suitable for larger networks that require longer distances.

Bandwidth sharing: Ethernet networks share bandwidth among all connected devices, which can result in reduced network speeds as the number of devices increases.

Security vulnerabilities: Although Ethernet includes built-in security features, it is still vulnerable to security breaches, including unauthorized access and data interception.

Complexity: Ethernet networks can be complex to set up and maintain, requiring specialized knowledge and expertise.

Compatibility issues: While Ethernet is generally interoperable with other networking technologies, compatibility issues can arise when integrating with older or legacy systems.

Cable installation: Ethernet networks require the installation of physical cables, which can be time-consuming and expensive to install.

Physical limitations: Ethernet networks require physical connections between devices, which can limit mobility and flexibility in network design.

How Ethernet Works?

In the Open Systems Interconnection (OSI) model, the Ethernet is located in the lower layers and facilitates the operation of the physical and data link layers. The OSI model consists of seven layers, which are as follows.

The topmost layer, known as the application layer, is what enables users to download and access data from email clients or web browsers. With the aid of the application, users enter their queries, and the request is then sent to the following layer, which is known as a "packet." The packet contains data about the sender and the destination web address. The packet is transmitted from the application layer until it reaches the bottom layer, also known as the Ethernet frame.

Comment More info Advertise with us

Next Article

Bridges (local Internetworking device)

Similar Reads

1. What is Fast Ethernet?
2. Fast Ethernet
3. Switched Ethernet
4. 10-Gigabit Ethernet
5. What is Power Over Ethernet (POE)?
6. What is Minimum Ethernet Frame Size?
7. Uses of Ethernet
8. Metro Ethernet (MetroE)
9. Types of Ethernet Cable
10. What is IPX(Internetwork Packet Exchange)?

GeeksforGeeks

Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Registered Address:
K 061, Tower K, Gulshan Vivante
Apartment, Sector 137, Noida, Gautam
Buddh Nagar, Uttar Pradesh, 201305

What is MAC Address?

Last Updated : 30 Sep, 2024

To communicate or transfer data from one computer to another, we need an address. In computer networks, various types of addresses are introduced; each works at a different layer. A MAC address, which stands for Media Access Control Address, is a physical address that works at the Data Link Layer. In this article, we will discuss addressing a DLL, which is the MAC Address.

So, go through the article if you are eager to learn what is MAC address and its components.

Table of Content

- What is MAC (Media Access Control) Address?
- Format of MAC Address
- Types of MAC Address
- Reason to have both IP and MAC addresses.
- Why should the MAC address be unique in the LAN network?
- How do I find the MAC Address?
- What is MAC Cloning?
- Characteristics of MAC Address
- Advantages of MAC Address
- Disadvantages of MAC Address

What is MAC (Media Access Control) Address?

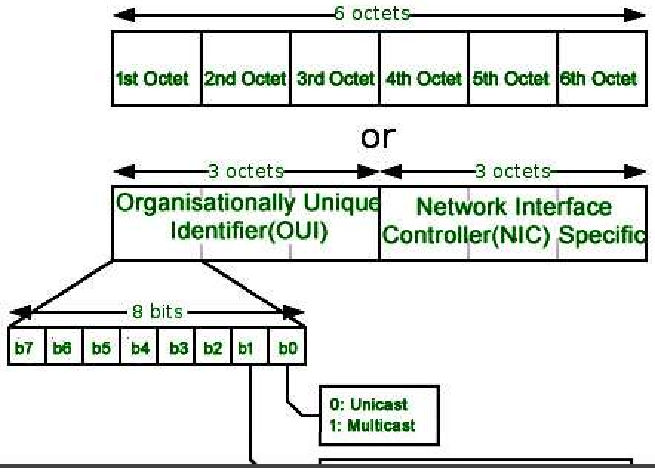
MAC Addresses are unique **48-bit** hardware numbers of a computer that are embedded into a network card (known as a **Network Interface Card**) during manufacturing. The MAC Address is also known as the **Physical**

Address of a network device. In the IEEE 802 standard, the data link layer is divided into two sublayers:

1. Logical Link Control (LLC) Sublayer
2. Media Access Control (MAC) Sublayer

The MAC address is used by the Media Access Control (MAC) sublayer of the Data-Link Layer. MAC Address is worldwide unique since millions of network devices exist and we need to uniquely identify each.

A **MAC address** uniquely identifies network interfaces. For more on networking fundamentals and concepts like MAC addresses, the GATE CS Self-Paced Course is a comprehensive guide.


6 octets
1st Octet
2nd Octet
3rd Octet
4th Octet
5th Octet
6th Octet
or
3 octets
3 octets
Organisationally Unique Identifier(OUI)
Network Interface Controller(NIC) Specific
8 bits
b7
b6
b5
b4
b3
b2
b1
b0
0: Unicast
1: Multicast

Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw

Format of MAC Address

To understand what is MAC address is, it is very important that first you understand the format of the MAC Address. So a MAC Address is a 12-digit hexadecimal number (48-bit binary number), which is mostly represented by Colon-Hexadecimal notation.

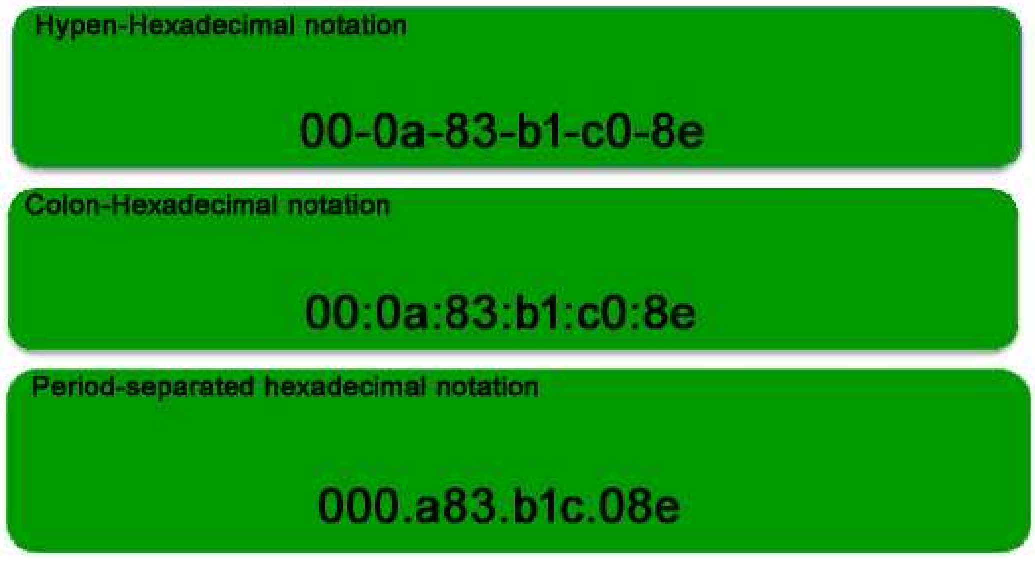
The First 6 digits (say 00:40:96) of the MAC Address identify the manufacturer, called the OUI (**Organizational Unique Identifier**). IEEE Registration Authority Committee assigns these MAC prefixes to its registered vendors.

Here are some OUI of well-known manufacturers:

```
CC:46:D6 - Cisco
3C:5A:B4 - Google, Inc.
3C:D9:2B - Hewlett Packard
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD
```

The rightmost six digits represent **Network Interface Controller**, which is assigned by the manufacturer.

As discussed above, the MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory. MAC address can be represented using any of the following formats:



Hypen-Hexadecimal notation
00-0a-83-b1-c0-8e

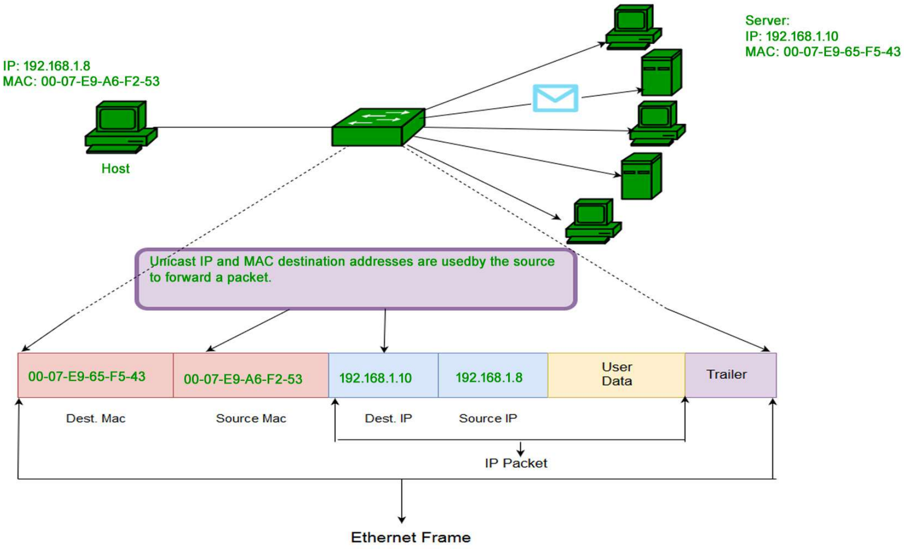
Colon-Hexadecimal notation
00:0a:83:b1:c0:8e

Period-separated hexadecimal notation
000.a83.b1c.08e

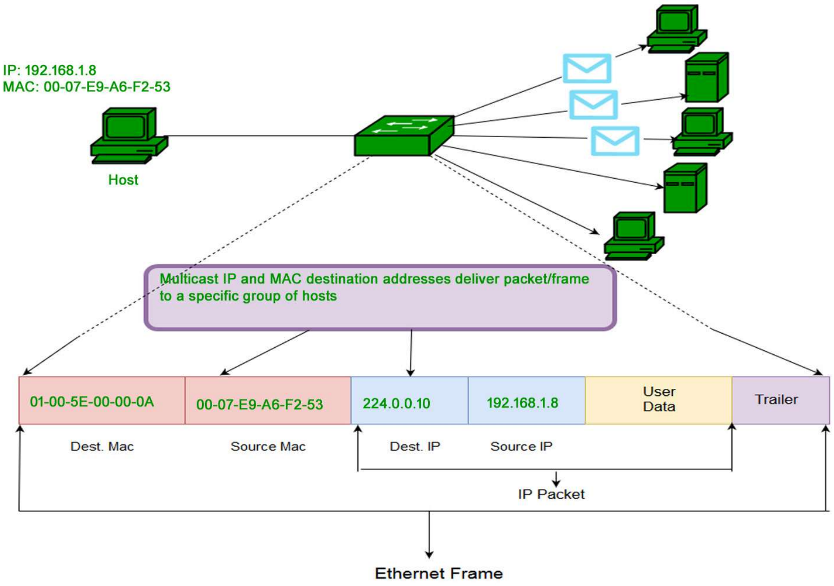
Note: Colon-Hexadecimal notation is used by *Linux OS* and Period-separated Hexadecimal notation is used by *Cisco Systems*.

Types of MAC Address

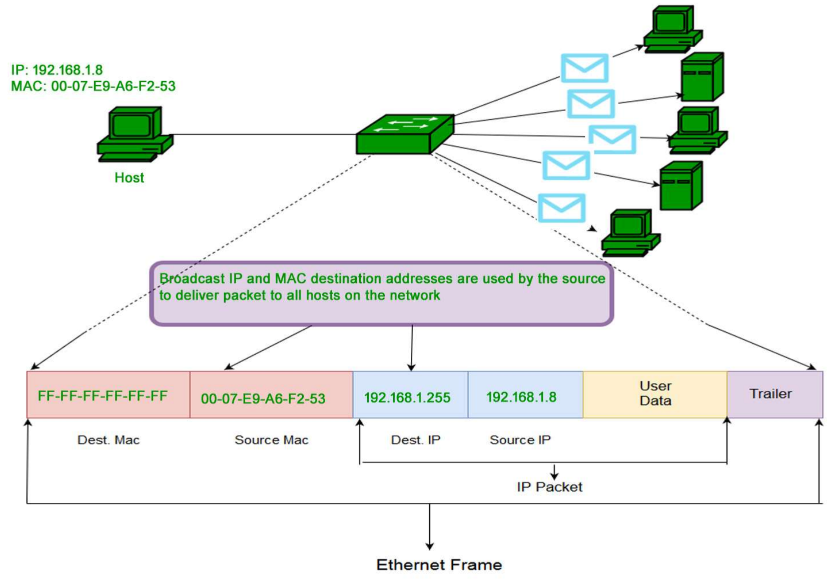
1. Unicast: A Unicast-addressed frame is only sent out to the interface leading to a specific NIC. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. The MAC Address of the source machine is always Unicast.


IP: 192.168.1.8
MAC: 00-07-E9-A6-F2-53
Host
Server:
IP: 192.168.1.10
MAC: 00-07-E9-65-F5-43
Unicast IP and MAC destination addresses are usedby the source to forward a packet.
00-07-E9-65-F5-43
00-07-E9-A6-F2-53
192.168.1.10
192.168.1.8
User Data
Trailer
Dest. Mac
Source Mac
Dest. IP
Source IP
IP Packet
Ethernet Frame

2. Multicast: The multicast address allows the source to send a frame to a group of devices. In Layer-2 (Ethernet) Multicast address, the LSB (least significant bit) of the first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.


IP: 192.168.1.8
MAC: 00-07-E9-A6-F2-53
Host
Multicast IP and MAC destination addresses deliver packet/frame to a specific group of hosts
01-00-5E-00-00-0A
00-07-E9-A6-F2-53
224.0.0.10
192.168.1.8
User Data
Trailer
Dest. Mac
Source Mac
Dest. IP
Source IP
IP Packet
Ethernet Frame

3. Broadcast: Similar to Network Layer, Broadcast is also possible on the underlying layer(Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred to as the broadcast addresses. Frames that are destined with MAC address FF-FF-FF-FF-FF-FF will reach every computer belonging to that LAN segment.


IP: 192.168.1.8
MAC: 00-07-E9-A6-F2-53
Host
Broadcast IP and MAC destination addresses are used by the source to deliver packet to all hosts on the network
FF-FF-FF-FF-FF-FF
00-07-E9-A6-F2-53
192.168.1.255
192.168.1.8
User Data
Trailer
Dest. Mac
Source Mac
Dest. IP
Source IP
IP Packet
Ethernet Frame

Reason to Have Both IP and MAC Addresses.

The reason for having both IP and MAC addresses lies in the way the Internet works, specifically in the structure of the OSI Model. This model is a conceptual framework that describes how data is sent and received over a network. It's divided into seven layers, each performing specific functions.

- **Layer 2** uses **MAC addresses** and is responsible for packet delivery from **hop to hop** .
- **Layer 3** uses **IP addresses** and is responsible for packet delivery from **end to end** .

Layer 2 **(Data Link Layer)** uses a **MAC (Media Access Control) address**. These are unique identifiers assigned to network interfaces for communications at the data link layer. The primary function of MAC addresses is to manage how data is transported from one network node to another on a direct, physical basis - this is also referred to as "hop to hop" delivery.

On the other hand, Layer 3 **(Network Layer)** uses an **IP (Internet Protocol) address**. These IP addresses are used to identify devices on a network and to route traffic between networks. The IP addresses ensure that the data gets from its original source reaches its final destination and it is also called "end-to-end" delivery of data.

When a computer sends data, it first wraps it in an IP header, which includes the source and destination IP addresses. This IP header, along with the data, is then encapsulated in a MAC header, which includes the source and destination MAC addresses for the current "hop" in the path.

As the data travels from one router to the next, the MAC address header is stripped off and a new one is generated for the next hop. However, the IP header, which was generated by the original computer, remains intact until it reaches the final destination. This process illustrates how the IP header manages the "end to end" delivery, while the MAC headers handle the "hop to hop" delivery.

So, Both IP and MAC addresses are essential for the functioning of the Internet. While MAC addresses facilitate the direct, physical transfer of data between network nodes, IP addresses ensure that the data reaches its final destination.

Why Should the MAC Address Be Unique in the LAN Network?

Consider a **LAN** (**Local Area Network**) as a large gathering where everyone is engaged in conversations. Now, let's suppose that there are two individuals at this gathering who coincidentally share the same name. This scenario would inevitably create confusion, right? If someone calls out that name, both individuals would respond, making it challenging to discern the intended recipient of the message.

In a similar manner, within a network, each device possesses a distinct identifier referred to as a MAC (Media Access Control) address. Think of it as a unique name assigned to the device. When information is transmitted across the network, it is directed to a specific MAC address, much like a letter being addressed to a specific individual.

However, if multiple devices within the same network were to have identical MAC addresses, it would result in confusion and disrupt the network's functioning. The network would struggle to ascertain which device should receive the transmitted information. To prevent this confusion and ensure the accurate delivery of information, it is vital for each device on a network to possess a unique MAC address.

How Do I Find the MAC Address?

A MAC address is mostly used to configure a router for a network device or during troubleshooting. The address of our computer device can be easily checked with any operating device. All the Apple devices connected to our home network contain a unique MAC address. Manufacturers may identify a MAC address by other names, such as the physical address, hardware ID, wireless ID, and Wi-Fi address.

Following are the steps which help to find MAC addresses for different OS

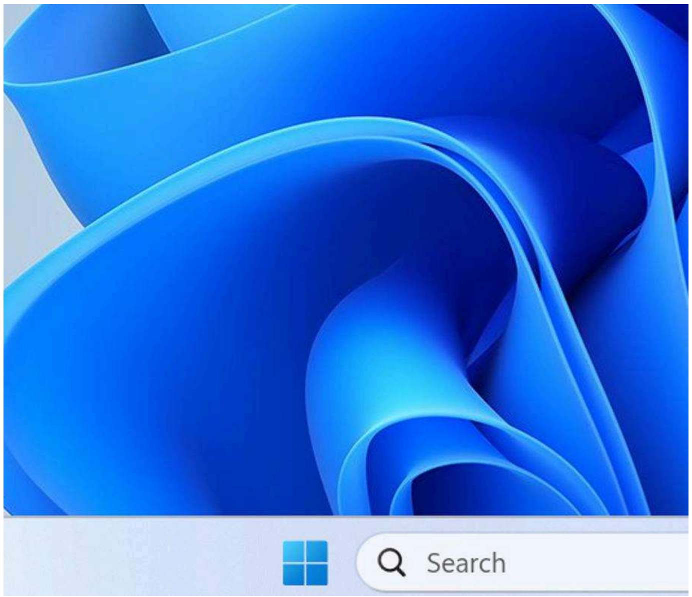
MAC address on Windows

Here is the Step-by-Step guide to finding MAC addresses on Windows.

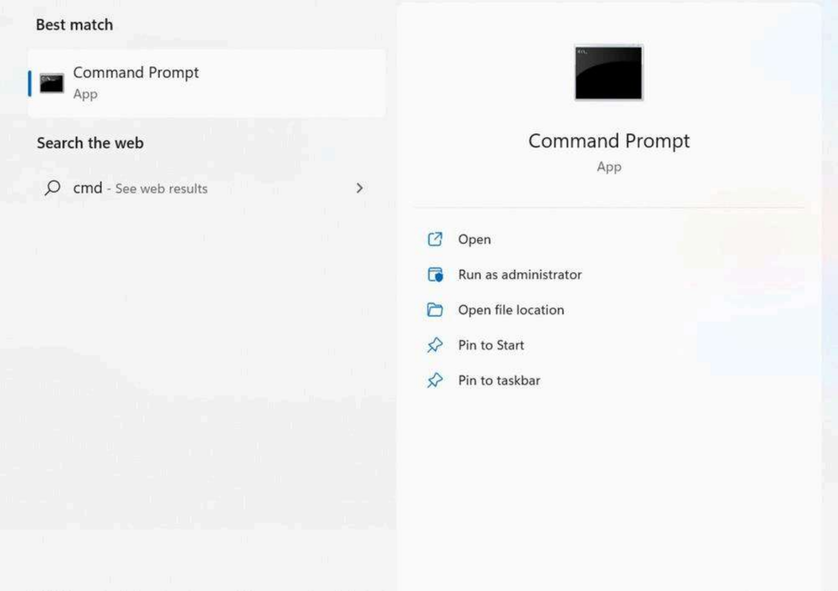
Command:

```
ipconfig /all
```

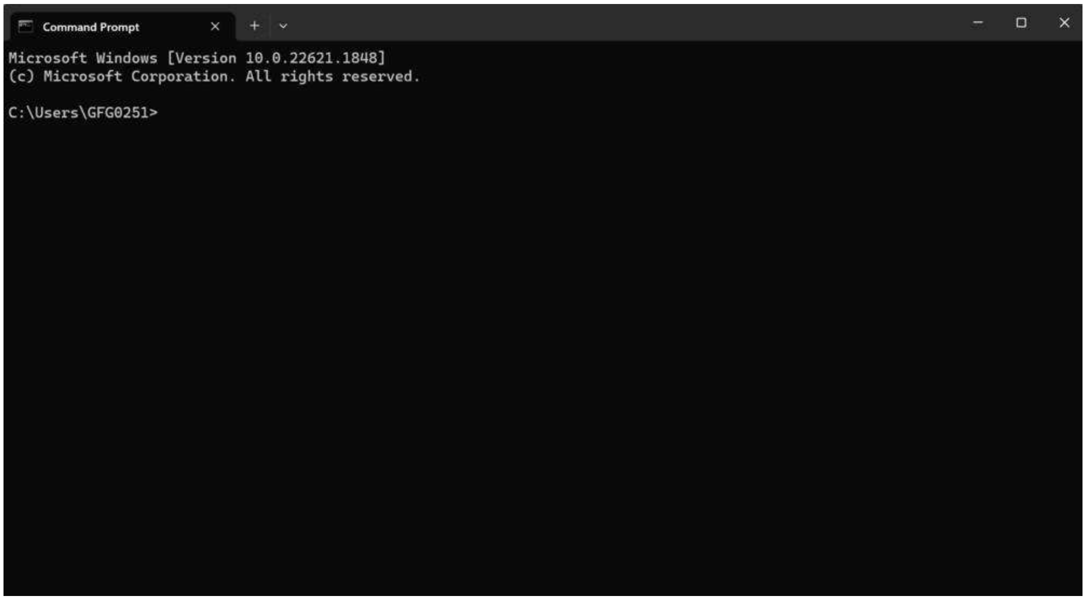
Step 1 - Press **Window Start** or Click on Windows Key.



Step 2 - In the search box, type **cmd,** and the command prompt will get open.

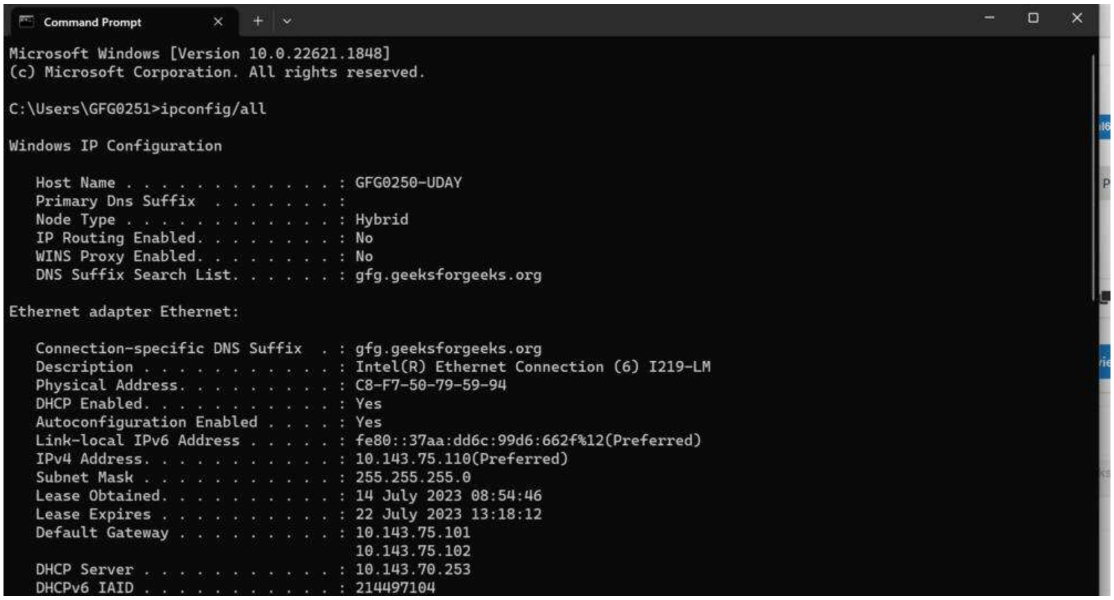

Best match
Command Prompt
App
Search the web
cmd - See web results
Command Prompt
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar

Step 3 - Click on cmd, the command prompt window will display,



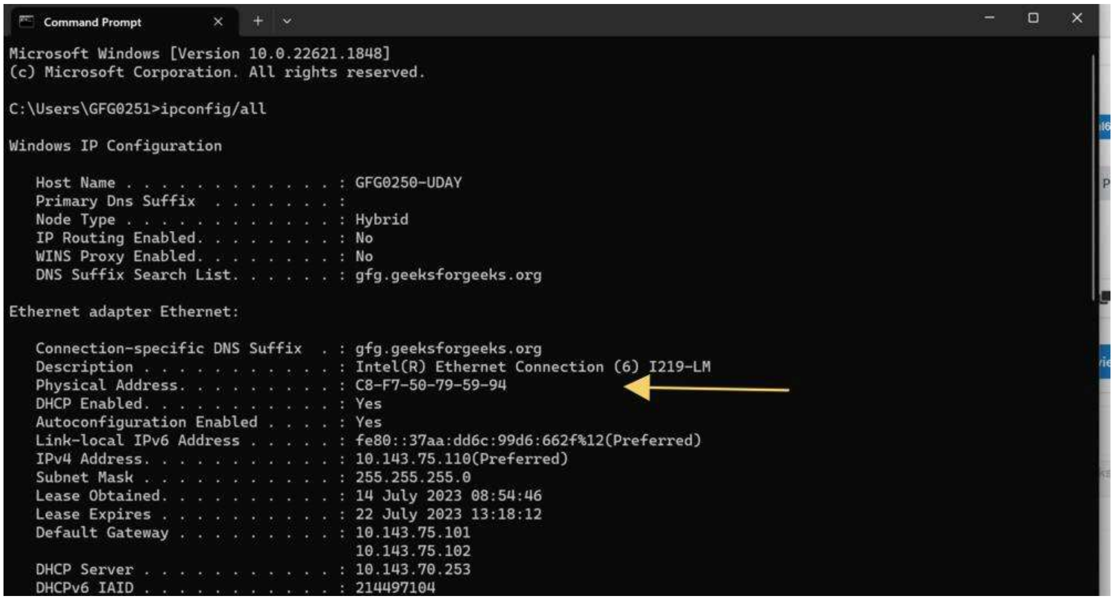
```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\GFG0251>
```

Step 4 - In the command prompt type **ipconfig/all** command and then press enter.



```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\GFG0251>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : GFG0250-UDAY
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : gfg.geeksforgeeks.org

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : gfg.geeksforgeeks.org
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (6) I219-LM
   Physical Address. . . . . . . . . : C8-F7-50-79-59-94
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::37aa:dd6c:99d6:662f%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.143.75.110(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 14 July 2023 08:54:46
   Lease Expires . . . . . . . . . . : 22 July 2023 13:18:12
   Default Gateway . . . . . . . . . : 10.143.75.101
                                       10.143.75.102
   DHCP Server . . . . . . . . . . . : 10.143.70.253
   DHCPv6 IAID . . . . . . . . . . . : 214497104
```

Step 5 - As you will scroll down, each physical address is the MAC address of your device.


Command Prompt

```
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Users\GFG0251>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : GFG0250-UDAY
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : gfg.geeksforgeeks.org

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : gfg.geeksforgeeks.org
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (6) I219-LM
   Physical Address. . . . . . . . . : C8-F7-50-79-59-94
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::37aa:dd6c:99d6:662f%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.143.75.110(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 14 July 2023 08:54:46
   Lease Expires . . . . . . . . . . : 22 July 2023 13:18:12
   Default Gateway . . . . . . . . . : 10.143.75.101
                                       10.143.75.102
   DHCP Server . . . . . . . . . . . : 10.143.70.253
   DHCPv6 IAID . . . . . . . . . . . : 214497104
```

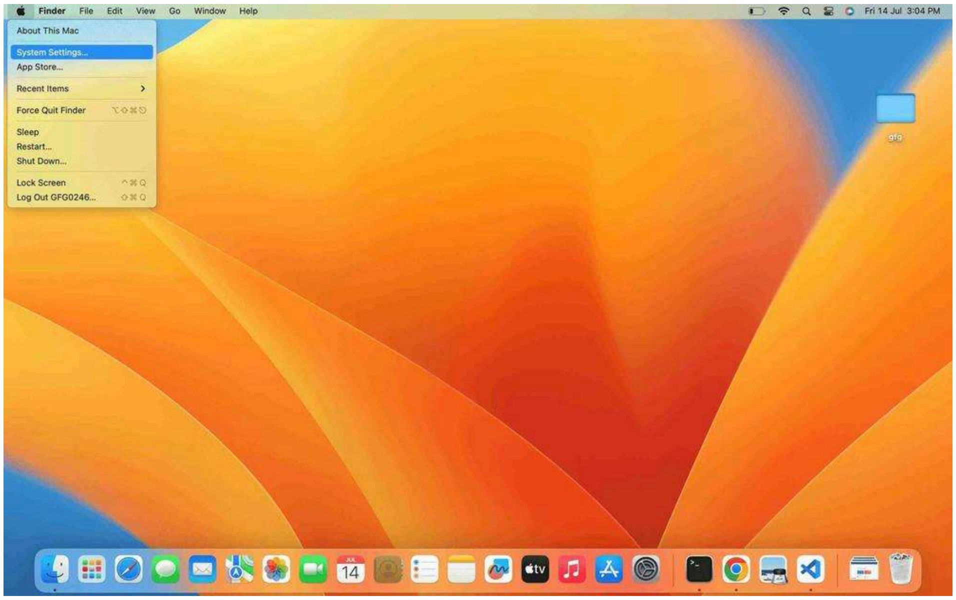
MAC Address on MacOS

Here is a step-by-step guide to finding MAC addresses on a Mac operating system.

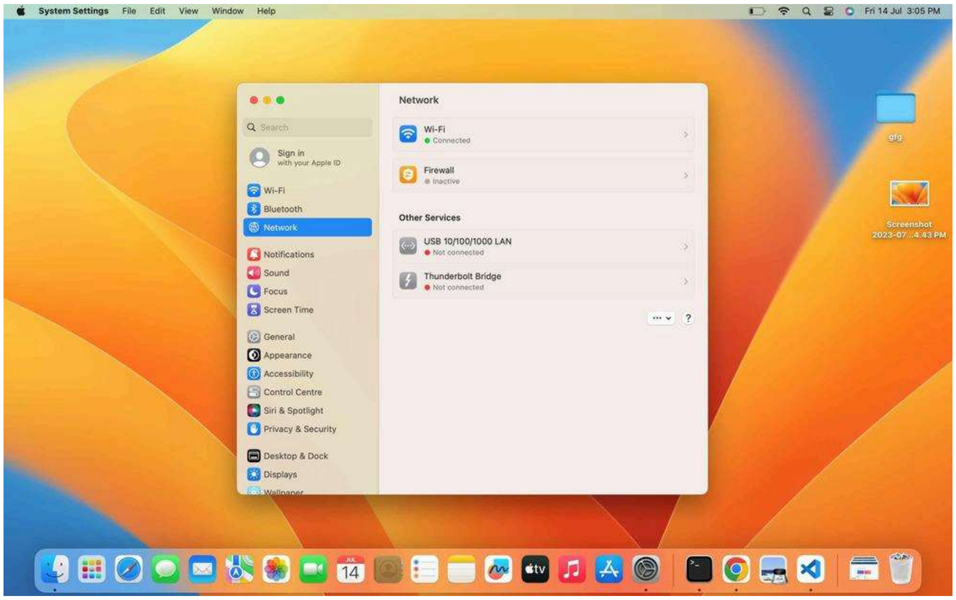
Command for MAC Address in MacOS:

```
TCP/IP Control Panel
```

Step 1 - Click on System Settings.


Finder
File
Edit
View
Go
Window
Help
Fri 14 Jul 3:04 PM
About This Mac
System Settings...
App Store...
Recent Items
Force Quit Finder
Sleep
Restart...
Shut Down...
Lock Screen
Log Out GFG0246...
gfg

Step 2 - In the system settings, click on the **MAC network** option.


System Settings File Edit View Window Help
Fri 14 Jul 3:05 PM
Search
Sign in with your Apple ID
Wi-Fi
Bluetooth
Network
Notifications
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Centre
Siri & Spotlight
Privacy & Security
Desktop & Dock
Displays
Wallpaper
gfg
Screenshot 2023-07...4.43 PM

Network

Wi-Fi ● Connected

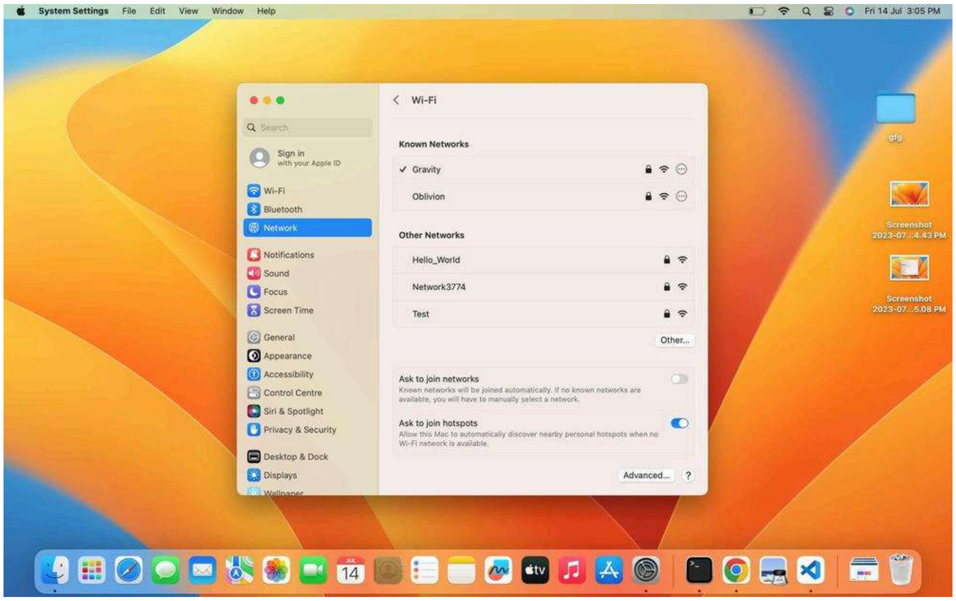
Firewall ● Inactive

Other Services

USB 10/100/1000 LAN ● Not connected

Thunderbolt Bridge ● Not connected

Step 3 - Then go to the **advanced settings.**


System Settings File Edit View Window Help
Fri 14 Jul 3:05 PM
Search
Sign in with your Apple ID
Wi-Fi
Bluetooth
Network
Notifications
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Centre
Siri & Spotlight
Privacy & Security
Desktop & Dock
Displays
Wallpaper
gfg
Screenshot 2023-07...4.43 PM
Screenshot 2023-07...5.08 PM
Other...
Advanced...
?

Wi-Fi

Known Networks

✓ Gravity

Oblivion

Other Networks

Hello_World

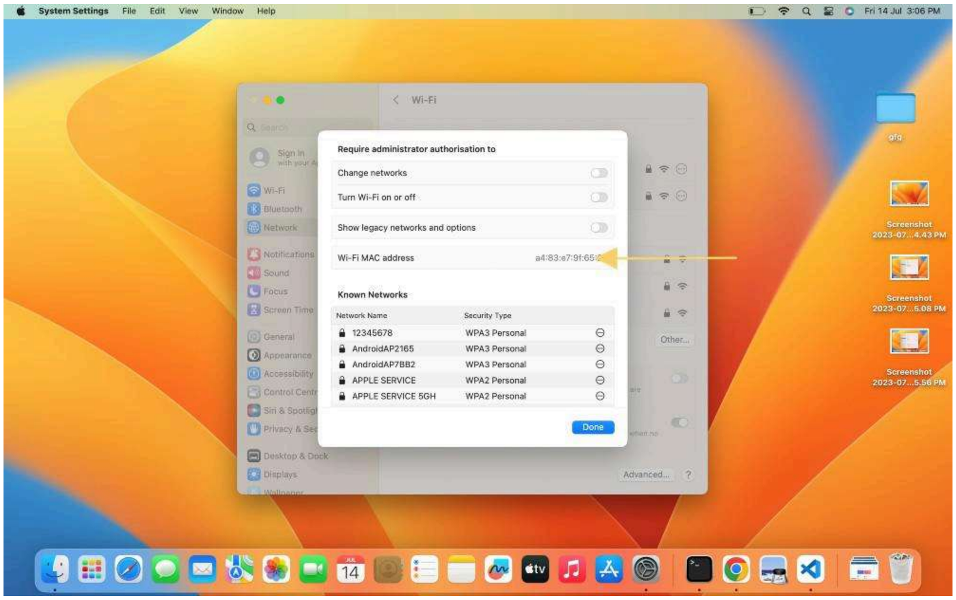
Network3774

Test

Ask to join networks
Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

Ask to join hotspots
Allow this Mac to automatically discover nearby personal hotspots when no Wi-Fi network is available.

Step 4 - Here you find your MAC address.


System Settings
File
Edit
View
Window
Help
Fri 14 Jul 3:06 PM
Wi-Fi
Search
Sign in with your A
Wi-Fi
Bluetooth
Network
Notifications
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Centr
Siri & Spotlig
Privacy & Se
Desktop & Dock
Displays
Other...
Advanced...
?
Done
ofg
Screenshot 2023-07...4.43 PM
Screenshot 2023-07...5.08 PM
Screenshot 2023-07...5.56 PM

Require administrator authorisation to

Change networks ○

Turn Wi-Fi on or off ○

Show legacy networks and options ○

Wi-Fi MAC address a4:83:e7:9f:65:

Known Networks

Network Name	Security Type
12345678	WPA3 Personal
AndroidAP2165	WPA3 Personal
AndroidAP7BB2	WPA3 Personal
APPLE SERVICE	WPA2 Personal
APPLE SERVICE 5GH	WPA2 Personal

MAC Address on Unix/Linux

Here is a step-by-step guide to finding MAC addresses on a Unix/Linux operating system.

Command For MAC Address in Unix/Linux:

```
ifconfig -a
ip link list
ip address show
```

__mask-blockquote__index=1__

What is MAC Cloning?

Some ISPs use MAC addresses to assign an IP address to the gateway device. When a device connects to the ISP, the DHCP server records the MAC address and then assigns an IP address. Now the system will be identified through the MAC address. When the device gets disconnected, it loses the IP address.

If the user wants to reconnect, the DHCP server checks if the device is connected before. If so, then the server tries to assign the same IP address (in case the lease period has not expired). In case the user changed the router, the user has to inform the ISP about the new MAC address because the new MAC address is unknown to ISP, so the connection cannot be established.

Or the other option is **Cloning**, user can simply clone the registered MAC address with ISP. Now router keeps reporting the old MAC addresses to ISP and there will be no connection issue.

Characteristics of MAC Address

The Media Access Control address (MAC address) is a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification and use in the Media Access Control protocol sub-layer.

An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits (4 bits per hexadecimal digit). MAC addresses are in a flat structure and thus they are not routable on the Internet. Serial interfaces do not use MAC addresses. It does NOT contain a network and host portion with the address. It is used to deliver the frame to the destination device.

- MAC addresses are used in LAN (Local Area Network) environments to identify devices and allow communication between them.
- MAC addresses are burned into the hardware of a network interface card (NIC) and cannot be changed, except in some rare cases where the manufacturer has provided a specific tool to do so.
- The first 3 bytes of a MAC address represent the manufacturer ID, while the last 3 bytes represent a unique identifier assigned by the manufacturer.
- MAC addresses are often used in conjunction with ARP (Address Resolution Protocol) to resolve IP addresses to MAC addresses for communication on a LAN.
- Some operating systems, such as Windows and Linux , allow you to view the MAC address of your network adapter through a command prompt or network settings.

Advantages of MAC Address

1. **Uniqueness:** Each MAC address is unique, which means that devices on the network can be easily identified and managed.
2. **Simplicity:** MAC addresses are easy to configure and manage, and do not require any additional network infrastructure.
3. **Compatibility:** MAC addresses are widely used and supported by a variety of networking technologies and protocols, making them compatible with many different systems.
4. **Security:** MAC addresses can be used to restrict access to a network by only allowing devices with authorized MAC addresses to connect.
5. **Fault-tolerance:** In case of hardware or software failure, a device can be easily replaced without affecting the network, as long as the new device has the same MAC address as the old one.
6. **Multicasting:** MAC addresses can be used for multicasting, allowing a single packet to be sent to multiple devices at once.
7. **Efficiency:** MAC addresses allow for efficient communication on the network, as they enable devices to quickly and easily identify and communicate with each other.
8. **Lower network overhead:** MAC addresses reduce network overhead by allowing devices to communicate directly with each other without the need for additional routing or addressing.
9. **Ease of troubleshooting:** MAC addresses can be used to troubleshoot network issues by identifying the source of problems and tracking network activity.
10. **Flexibility:** MAC addresses can be used to support a variety of network configurations and topologies, including peer-to-peer, client-server, and hybrid models.

Disadvantages of MAC Address

1. **Limited address space:** MAC addresses are 48-bit numbers, which means that there is a finite number of possible MAC addresses. This can lead to address conflicts if multiple devices have the same MAC address.

2. **Spoofing:** MAC addresses can be easily spoofed, allowing unauthorized devices to gain access to the network.
3. **Inefficiency:** MAC addresses are not hierarchical, which can make it difficult to efficiently manage large networks.
4. **Static addressing:** MAC addresses are typically assigned at the time of manufacture and cannot be easily changed. This can be a disadvantage in situations where devices need to be reconfigured or replaced.
5. **Limited scope:** MAC addresses are only used for identifying devices within a local network segment, and cannot be used to identify devices outside of this segment.
6. **Hardware-dependent:** MAC addresses are tied to the network interface card (NIC) of a device, which means that if the NIC fails or is replaced, the MAC address also changes.
7. **Lack of encryption:** MAC addresses are sent in plain text, which can make them vulnerable to interception and eavesdropping.
8. **No inherent security:** While MAC filtering can be used to restrict access to a network, MAC addresses themselves do not provide any inherent security features.
9. **MAC address collisions:** In rare cases, MAC addresses can collide, which can cause network disruptions and make it difficult to identify and manage devices on the network.

Comment More info Advertise with us

Next Article

What is an IP Address?

Similar Reads

1. What is MAC Address Table ?
2. What is Public IP Address?
3. What is a Network Address?
4. What is Limited Broadcast Address?
5. What is External IP Address?

Carrier Sense Multiple Access (CSMA)

Last Updated : 09 Oct, 2024

Carrier Sense Multiple Access (CSMA) is a method used in computer networks to manage how devices share a communication channel to transfer the data between two devices. In this protocol, each device first sense the channel before sending the data. If the channel is busy, the device waits until it is free. This helps reduce collisions, where two devices send data at the same time, ensuring smoother communication across the network. CSMA is commonly used in technologies like Ethernet and Wi-Fi.

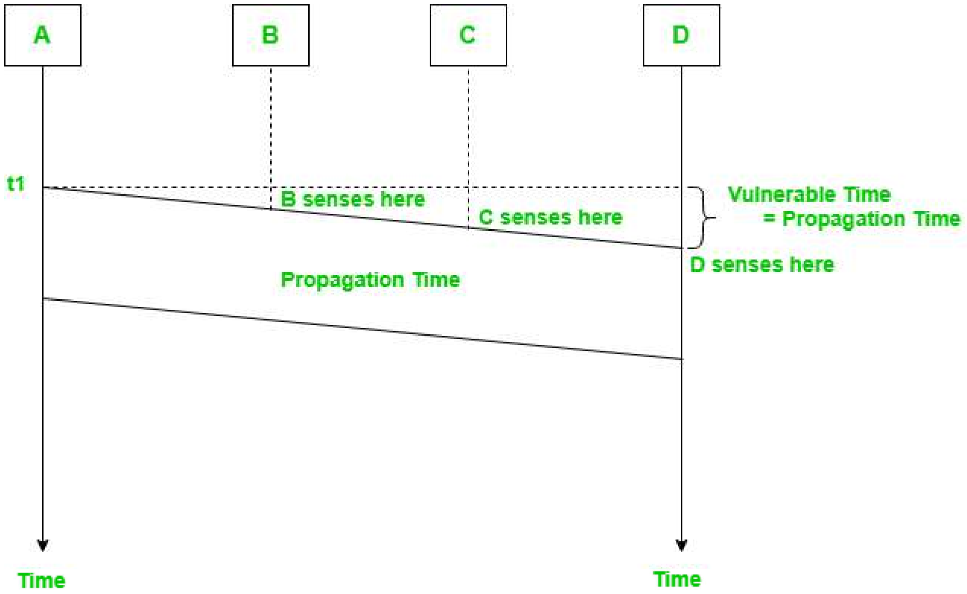
This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.

What is Vulnerable Time in CSMA?

Vulnerable time is the short period when there’s a chance that two devices on a network might send data at the same time and cause a collision.

In networks like Wi-Fi or Ethernet, devices first listen to see if the network is clear before sending their data. However, after a device checks and finds the network free, there’s a small delay before it starts sending data. During this time, another device might also try to send data, which can lead to both data packets crashing into each other (a collision). This period, where a collision might happen, is called the **vulnerable time**.

```
Vulnerable time = Propagation time (Tp)
```


A
B
C
D
t1
B senses here
C senses here
D senses here
Vulnerable Time
= Propagation Time
Propagation Time
Time
Time

when the channel is busy/idle.

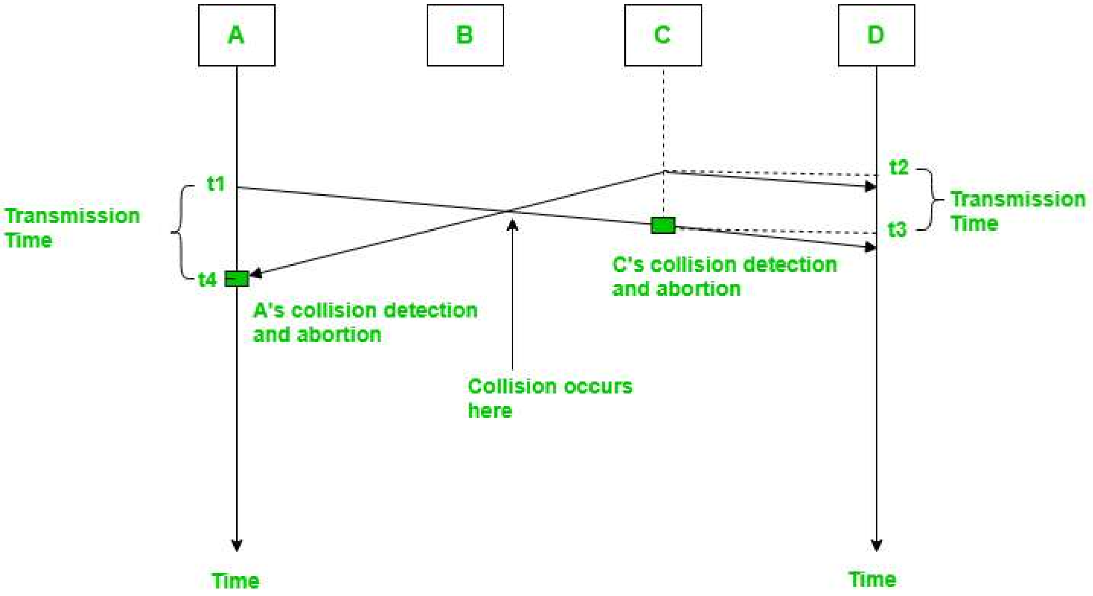
Types of CSMA Protocol

There are two main types of **Carrier Sense Multiple Access (CSMA)** protocols, each designed to handle how devices manage potential data collisions on a shared communication channel. These types differ based on how they respond to the detection of a busy network:

1. CSMA/CD
2. CSMA/CA

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

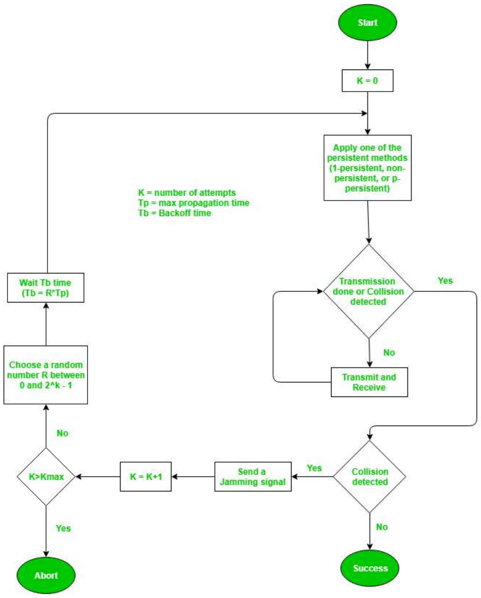
In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the transmission is finished, if not, the frame is sent again.


A
B
C
D
t1
t4
Transmission Time
t2
t3
Transmission Time
C's collision detection and abortion
A's collision detection and abortion
Collision occurs here
Time
Time

In the diagram, *starts* sending the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is, therefore, t3-t2 and for A's frame is t4-t1

So, the **frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp)**. This can be deduced when the two stations involved in a collision are a maximum distance apart.

Process: The entire process of collision detection can be explained as follows:


Start
K = 0
Apply one of the persistent methods (1-persistent, non-persistent, or p-persistent)
K = number of attempts
Tp = max propagation time
Tb = Backoff time
Transmission done or Collision detected
Yes
No
Transmit and Receive
Wait Tb time (Tb = R*Tp)
Choose a random number R between 0 and 2^k - 1
No
K>Kmax
K = K+1
Send a Jamming signal
Yes
Collision detected
Yes
No
Abort
Success

Throughput and Efficiency: The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

- For the 1-persistent method, throughput is 50% when G=1.
- For the non-persistent method, throughput can go up to 90%.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of the received signal almost doubles, and the station can sense the possibility of collision. In the case of wireless networks, most of the energy is used for transmission, and the energy of the received signal increases by only 5-10% if a collision occurs. It can't be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

These are three types of strategies:

1. **InterFrame Space (IFS):** When a station finds the channel busy it senses the channel again, when the station finds a channel to be idle it waits for a period of time called **IFS time**. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
2. **Contention Window:** It is the amount of time divided into slots. A station that is ready to send frames chooses a random number of slots as **wait time**.
3. **Acknowledgments:** The positive acknowledgments and time-out timer can help guarantee a successful transmission of the frame.

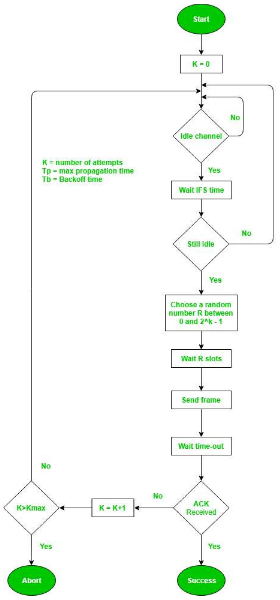
Characteristics of CSMA/CA

1. **Carrier Sense**: The device listens to the channel before transmitting, to ensure that it is not currently in use by another device.

2. **Multiple Access**: Multiple devices share the same channel and can transmit simultaneously.
3. **Collision Avoidance**: If two or more devices attempt to transmit at the same time, a collision occurs. CSMA/CA uses random backoff time intervals to avoid collisions.
4. **Acknowledgment (ACK)**: After successful transmission, the receiving device sends an ACK to confirm receipt.
5. **Fairness**: The protocol ensures that all devices have equal access to the channel and no single device monopolizes it.
6. **Binary Exponential Backoff**: If a collision occurs, the device waits for a random period of time before attempting to retransmit. The backoff time increases exponentially with each retransmission attempt.
7. **Interframe Spacing**: The protocol requires a minimum amount of time between transmissions to allow the channel to be clear and reduce the likelihood of collisions.
8. **RTS/CTS Handshake**: In some implementations, a Request-To-Send (RTS) and Clear-To-Send (CTS) handshake is used to reserve the channel before transmission. This reduces the chance of collisions and increases efficiency.
9. **Wireless Network Quality**: The performance of CSMA/CA is greatly influenced by the quality of the wireless network, such as the strength of the signal, interference, and network congestion.
10. **Adaptive Behavior**: CSMA/CA can dynamically adjust its behavior in response to changes in network conditions, ensuring the efficient use of the channel and avoiding congestion.

Overall, CSMA/CA balances the need for efficient use of the shared channel with the need to avoid collisions, leading to reliable and fair communication in a wireless network.

Process: The entire process of collision avoidance can be explained as follows:


Start
K = 0
No
Idle channel
K = number of attempts
Tp = max propagation time
Tb = Backoff time
Yes
Wait IFS time
No
Still idle
Yes
Choose a random number R between 0 and 2^k - 1
Wait R slots
Send frame
Wait time-out
No
No
K>Kmax
K = K+1
ACK Received
Yes
Yes
Abort
Success

Types of CSMA Access Modes

There are 4 types of access modes available in CSMA. It is also referred as 4 different types of CSMA protocols which decide the time to start sending data across shared media.

1. **1-Persistent:** It senses the shared channel first and delivers the data right away if the channel is idle. If not, it must wait and ***continuously*** track for the channel to become idle and then broadcast the frame without condition as soon as it does. It is an aggressive transmission algorithm.
2. **Non-Persistent:** It first assesses the channel before transmitting data; if the channel is idle, the node transmits data right away. If not, the station must wait for an arbitrary amount of time (***not continuously***), and when it discovers the channel is empty, it sends the frames.
3. **P-Persistent:** It consists of the 1-Persistent and Non-Persistent modes combined. Each node observes the channel in the 1Persistent mode, and if the channel is idle, it sends a frame with a P probability. If the data is not transferred, the frame restarts with the following time slot after waiting for a (q = 1-p probability) random period.
4. **O-Persistent:** A supervisory node gives each node a transmission order. Nodes wait for their time slot according to their allocated transmission sequence when the transmission medium is idle.

Advantages of CSMA

- **Increased Efficiency:** CSMA ensures that only one device communicates on the network at a time, reducing collisions and improving network efficiency.
- **Simplicity:** CSMA is a simple protocol that is easy to implement and does not require complex hardware or software.
- **Flexibility:** CSMA is a flexible protocol that can be used in a wide range of network environments, including wired and wireless networks.
- **Low cost:** CSMA does not require expensive hardware or software, making it a cost-effective solution for network communication.

Disadvantages of CSMA

- **Limited Scalability:** CSMA is not a scalable protocol and can become inefficient as the number of devices on the network increases.
- **Delay:** In busy networks, the requirement to sense the medium and wait for an available channel can result in delays and increased latency.
- **Limited Reliability:** CSMA can be affected by interference, noise, and other factors, resulting in unreliable communication.
- **Vulnerability to Attacks:** CSMA can be vulnerable to certain types of attacks, such as jamming and denial-of-service attacks, which can disrupt network communication.

Comparisonof Various Protocols

Protocol	Transmission behavior	Collision detection method	Efficiency	Use cases
Pure ALOHA	Sends frames immediately	No collision detection	Low	Low-traffic networks

Protocol	Transmission behavior	Collision detection method	Efficiency	Use cases
Slotted ALOHA	Sends frames at specific time slots	No collision detection	Better than pure ALOHA	Low-traffic networks
CSMA/CD	Monitors medium after sending a frame, retransmits if necessary	Collision detection by monitoring transmissions	High	Wired networks with moderate to high traffic
CSMA/CA	Monitors medium while transmitting, adjusts behavior to avoid collisions	Collision avoidance through random backoff time intervals	High	Wireless networks with moderate to high traffic and high error rates

Conclusion

In conclusion, **Carrier Sense Multiple Access (CSMA)** is a method used by devices in a network to share the communication channel without causing too many collisions. It works by having each device listen to the channel before sending data. CSMA/CD (Collision Detection) is used mostly in wired networks like Ethernet. It listens for collisions during transmission and, if a collision happens, devices stop sending, wait, and try again. CSMA/CA (Collision Avoidance) is commonly used in wireless networks like Wi-Fi. It focuses on preventing collisions before they happen by having devices wait for a random time or send signals before transmitting data.

Comment More info Advertise with us

Next Article

Collision Detection in CSMA/CD

Similar Reads

1. Virtual Time Carrier Sensed Multiple Access (VT-CSMA)
2. Multiple Access with Collision Avoidance (MACA)
3. Java | CDMA (Code Division Multiple Access)
4. Demand Assigned Multiple Access (DAMA) in Networking
5. Multiple Access Protocols in Computer Network
6. Frequency Division Multiple Access (FDMA) Techniques
7. Code Division Multiplexing
8. Wireless Media Access Issues in Internet of Things
9. Acquiring Channel in CSMA/CD
10. Difference Between CSMA/CA and CSMA/CD

GeeksforGeeks
Sanchhaya Education Private Limited

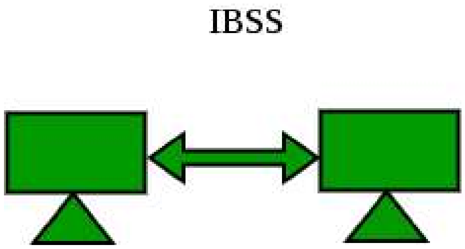
Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

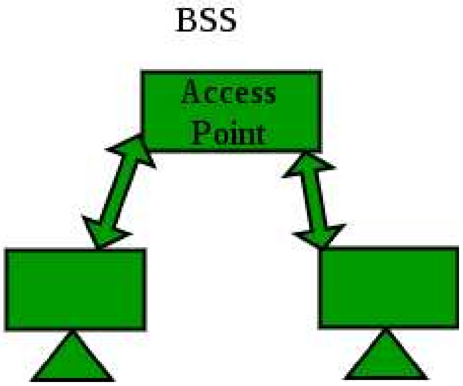
Registered Address:
K 061, Tower K, Gulshan Vivante
Apartment, Sector 137, Noida, Gautam
Buddh Nagar, Uttar Pradesh, 201305

Basics of Wi-Fi

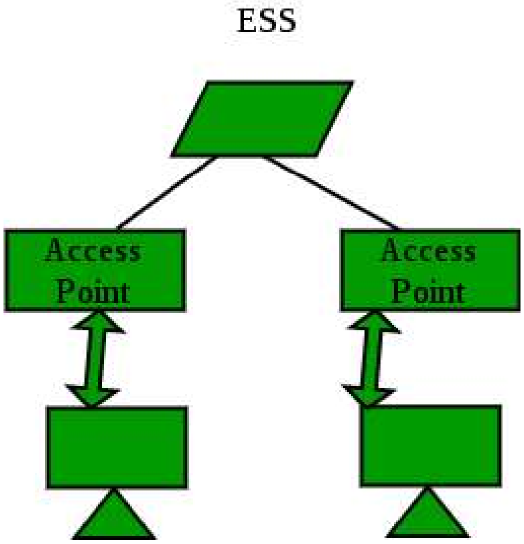
Last Updated : 25 Mar, 2023

We've been studying a lot about the Wired Network. Ethernet is the most common example. Wired networks differ from wireless which uses radio waves rather than transmitting electrical signals over the cables. Wi-Fi stands for Wireless Fidelity. It is a technology for wireless local area networking with devices based on IEEE 802.11 standards. Wi-Fi compatible devices can connect to the internet via WLAN network and a wireless **access point** abbreviated as AP. Every WLAN has an access point which is responsible for receiving and transmitting data from/to users. IEEE has defined certain specifications for wireless LAN, called **IEEE 802.11** which covers physical and data link layers. **Access Point(AP)** is a wireless LAN base station that can connect one or many wireless devices simultaneously to internet. The architecture of this standard has 2 kinds of services: **1. BSS (Basic Service Set) 2. ESS (Extended Service Set)** **BSS** is the basic building block of WLAN. It is made of wireless mobile stations and an optional central base station called Access Point. Stations can form a network without an AP and can agree to be a part of a BSS. A BSS without an AP cannot send data to other BSSs and defines a standalone network. It is called **Ad-hoc network** or **Independent BSS(IBSS).**i.e A BSS without AP is an ad-hoc network. A BSS with AP is **infrastructure network.** The figure below depicts an IBSS, BSS with the green coloured box depicting an AP.





ESS is made up of 2 or more BSSs with APs. BSSs are connected to the distribution system via their APs. The distribution system can be any IEEE LAN such as Ethernet.   ESS has 2 kinds of stations: 1. Mobile - stations inside the BSS 2. Stationary - AP stations that are part of wired LAN.



The topmost green box represents the distribution system and the other 2 green boxes represent the APs of 2 BSSs.

Features of Wi-Fi include:

Wireless Connectivity: Wi-Fi allows devices to connect to a network without the use of physical cables, providing greater mobility and flexibility.

High Speed: Wi-Fi networks can provide high-speed internet access, allowing users to download and upload data quickly.

Easy Setup: Wi-Fi networks are easy to set up and configure, requiring minimal technical knowledge. Most modern devices come with Wi-Fi connectivity built-in.

Multiple Device Connectivity: Wi-Fi networks can support multiple devices at the same time, allowing multiple users to connect to the same network and access the internet simultaneously.

Security: Wi-Fi networks can be secured using encryption and other security measures, which protect against unauthorized access and hacking.

Range: Wi-Fi networks can cover a wide range of distances, depending on the type of router and the environment in which it is used.

Compatibility: Wi-Fi is a widely adopted technology and is compatible with a wide range of devices, including smartphones, laptops, tablets, and smart home devices.

Interference: Wi-Fi signals can be subject to interference from other wireless devices and physical barriers, such as walls and buildings, which can impact network performance.

Reliability: Wi-Fi networks can sometimes suffer from dropouts or signal loss, particularly in areas with high network congestion or interference.

Comment More info Advertise with us

Next Article

The Internet and the Web

Similar Reads

1. What is Wi-Fi?
2. Wi-Fi Standards Explained
3. What is a Wireless Access Point?
4. WiFi and its Amendments
5. How to Hack a Open WiFi?
6. Risks Associated With Public Wi-Fi
7. Wireless Application Protocol
8. WiMax in Computer Network

Virtual LAN (VLAN)

Last Updated : 24 Mar, 2023

Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide the broadcast domain but the broadcast domain can be divided by switches

A broadcast domain is a network segment in which if a device broadcast a packet then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packets but it is limited to switches only as routers don't forward out the broadcast packet. To forward out the packets to different VLAN (from one VLAN to another) or broadcast domains, inter Vlan routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

VLAN ranges:

- **VLAN 0, 4095:** These are reserved VLAN which cannot be seen or used.
- **VLAN 1:** It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.
- **VLAN 2-1001:** This is a normal VLAN range. We can create, edit and delete these VLAN.
- **VLAN 1002-1005:** These are CISCO defaults for fddi and token rings. These VLAN can't be deleted.
- **Vlan 1006-4094:** This is the extended range of Vlan.

Configuration -

We can simply create VLANs by simply assigning the vlan-id and Vlan name.

```
#switch1(config)#vlan 2
#switch1(config-vlan)#vlan accounts
```

Here, 2 is the Vlan I'd and accounts is the Vlan name. Now, we assign Vlan to the switch ports.e.g-

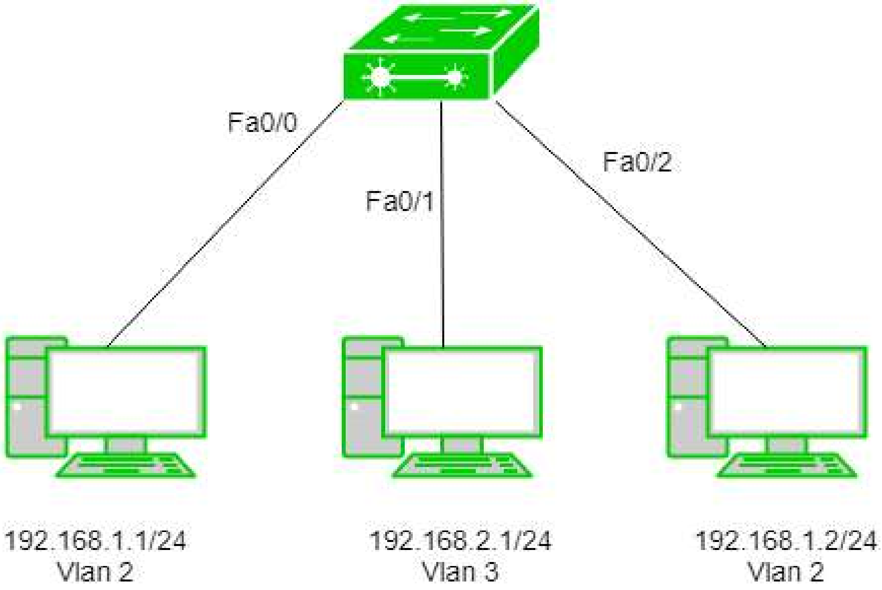
```
Switch(config)#int fa0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access Vlan 2
```

Also, switchport range can be assigned to required vlans.

```
Switch(config)#int range fa0/0-2
Switch(config-if)#switchport mode access
Switch(config-if) #switchport access Vlan 2
```

By this, switchport fa0/0, fa0/1, fa0-2 will be assigned Vlan 2.

Example -



Assigning IP address 192.168.1.1/24, 192.168.1.2/24 and 192.168.2.1/24 to the PC's. Now, we will create Vlan 2 and 3 on switch.

```
Switch(config)#vlan 2
Switch(config)#vlan 3
```

We have made VLANs but the most important part is to assign switch ports to the VLANs.

```
Switch(config)#int fa0/0
Switch(config-if)#switchport mode access
Switch(config-if) #switchport access Vlan 2

Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if) #switchport access Vlan 3

Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if) #switchport access Vlan 2
```

As seen, we have assigned Vlan 2 to fa0/0, fa0/2, and Vlan 3 to fa0/1.

VLANs offer several features and benefits, including:

- **Improved network security:** VLANs can be used to separate network traffic and limit access to specific network resources. This improves security by preventing unauthorized access to sensitive data and network resources.
- **Better network performance:** By segregating network traffic into smaller logical networks, VLANs can reduce the amount of broadcast traffic and improve network performance.
- **Simplified network management:** VLANs allow network administrators to group devices together logically, rather than physically, which can simplify network management tasks such as configuration, troubleshooting, and maintenance.
- **Flexibility:** VLANs can be configured dynamically, allowing network administrators to quickly and easily adjust network configurations as needed.

- **Cost savings:** VLANs can help reduce hardware costs by allowing multiple virtual networks to share a single physical network infrastructure.
- **Scalability:** VLANs can be used to segment a network into smaller, more manageable groups as the network grows in size and complexity.

Some of the key features of VLANs include:

- **VLAN tagging:** VLAN tagging is a way to identify and distinguish VLAN traffic from other network traffic. This is typically done by adding a VLAN tag to the Ethernet frame header.
- **VLAN membership:** VLAN membership determines which devices are assigned to which VLANs. Devices can be assigned to VLANs based on port, MAC address, or other criteria.
- **VLAN trunking:** VLAN trunking allows multiple VLANs to be carried over a single physical link. This is typically done using a protocol such as IEEE 802.1Q.
- **VLAN management:** VLAN management involves configuring and managing VLANs, including assigning devices to VLANs, configuring VLAN tags, and configuring VLAN trunking.

Types of connections in VLAN -

There are three ways to connect devices on a VLAN, the type of connections are based on the connected devices i.e. whether they are VLAN-aware(A device that understands VLAN formats and VLAN membership) or VLAN-unaware(A device that doesn't understand VLAN format and VLAN membership).

1. **Trunk Link -**
   All connected devices to a trunk link must be VLAN-aware. All frames on this should have a special header attached to it called tagged frames.
2. **Access link -**
   It connects VLAN-unaware devices to a VLAN-aware bridge. All frames

on the access link must be untagged.

3. **Hybrid link -**
   It is a combination of the Trunk link and Access link. Here both VLAN-unaware and VLAN-aware devices are attached and it can have both tagged and untagged frames.

Advantages -

- **Performance -**
  The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destinations. e.g.-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain, therefore, all will receive the traffic i.e. wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.
- **Formation of virtual groups -**
  As there are different departments in every organization namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.
- **Security -**
  In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.
- **Flexibility -**
  VLAN provide flexibility to add, remove the number of host we want.
- **Cost reduction -**
  VLANs can be used to create broadcast domains which eliminate the need for expensive routers.
  By using Vlan, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.

Disadvantages of VLAN

1. **Complexity:** VLANs can be complex to configure and manage, particularly in large or dynamic cloud computing environments.
2. **Limited scalability:** VLANs are limited by the number of available VLAN IDs, which can be a constraint in larger cloud computing environments.
3. **Limited security**: VLANs do not provide complete security and can be compromised by malicious actors who are able to gain access to the network.
4. **Limited interoperability**: VLANs may not be fully compatible with all types of network devices and protocols, which can limit their usefulness in cloud computing environments.
5. **Limited mobility**: VLANs may not support the movement of devices or users between different network segments, which can limit their usefulness in mobile or remote cloud computing environments.
6. **Cost:** Implementing and maintaining VLANs can be costly, especially if specialized hardware or software is required.
7. **Limited visibility:** VLANs can make it more difficult to monitor and troubleshoot network issues, as traffic is isolated in different segments.

Real-Time Applications of VLAN

Virtual LANs (VLANs) are widely used in cloud computing environments to improve network performance and security. Here are a few examples of real-time applications of VLANs:

1. **Voice over IP (VoIP)** : VLANs can be used to isolate voice traffic from data traffic, which improves the quality of VoIP calls and reduces the risk of network congestion.
2. **Video Conferencing** : VLANs can be used to prioritize video traffic and ensure that it receives the bandwidth and resources it needs for high-quality video conferencing.
3. **Remote Access** : VLANs can be used to provide secure remote access to cloud-based applications and resources, by isolating remote users

from the rest of the network.

4. **Cloud Backup and Recovery** : VLANs can be used to isolate backup and recovery traffic, which reduces the risk of network congestion and improves the performance of backup and recovery operations.
5. **Gaming** : VLANs can be used to prioritize gaming traffic, which ensures that gamers receive the bandwidth and resources they need for a smooth gaming experience.
6. **IoT** : VLANs can be used to isolate Internet of Things (IoT) devices from the rest of the network, which improves security and reduces the risk of network congestion.

Comment More info Advertise with us

Next Article

Configuring and Verifying VLANs in Cisco

Similar Reads

1. Types of Virtual LAN (VLAN)
2. VLAN ACL (VACL)
3. What is Virtual Channel?
4. VLAN Full Form
5. Native VLAN
6. Private VLAN
7. Hardware Based Virtualization
8. Creating Virtual Local Area Networks (VLANs) in Cisco
9. Difference between LAN and VLAN
10. Virtualization Fundamentals in CCNA

Stop and Wait ARQ

Last Updated : 11 Feb, 2025

Stop and Wait ARQ is a Sliding Window Protocol method used for the reliable delivery of data frames. The stop-and-wait ARQ is used for noisy channels or links to handle flow and error control between sender and receiver. The Stop and Wait ARQ protocol sends a data frame and then waits for an acknowledgment (ACK) from the receiver.

What is Stop and Wait ARQ?

The Stop and Wait ARQ protocol sends a data frame and then waits for an acknowledgment (ACK) from the receiver. The ACK indicates that the receiver successfully received the data frame. After receiving the ACK from the receiver, the sender delivers the next data frame. So there is a stop before the next data frame is transferred, hence it is known as the Stop and Wait ARQ protocol.

Characteristics of Stop and Wait ARQ

- Used in Connection-oriented communication.
- It offers error and flow control.
- It is used in Data Link and Transport Layers
- Stop and Wait for ARQ mainly implements the Sliding Window Protocol concept with Window Size 1
- It uses a link between sender and receiver as a half-duplex link
- Throughput = 1 Data packet/frame per RTT
- If the bandwidth*Delay product is very high, then they stop and wait for protocol if it is not so useful. The sender has to keep waiting for acknowledgments before sending the processed next packet.
- It is an example of "**Closed Loop OR connection-oriented** " protocols
- It is a special category of SWP where its window size is 1

- Irrespective of the number of packets sender is having stop and wait for protocol requires only 2 sequence numbers 0 and 1

Useful Terms in Stop and Wait Protocol

- **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.

Propagation Delay = (Distance between routers) / (Velocity of propagation)

- RoundTripTime **(RTT)** = Amount of time taken by a packet to reach the receiver + Time taken by the Acknowledgement to reach the sender
- TimeOut (**TO**) = 2* RTT
- Time To Live (**TTL**) = 2* TimeOut. (Maximum TTL is 255 seconds)

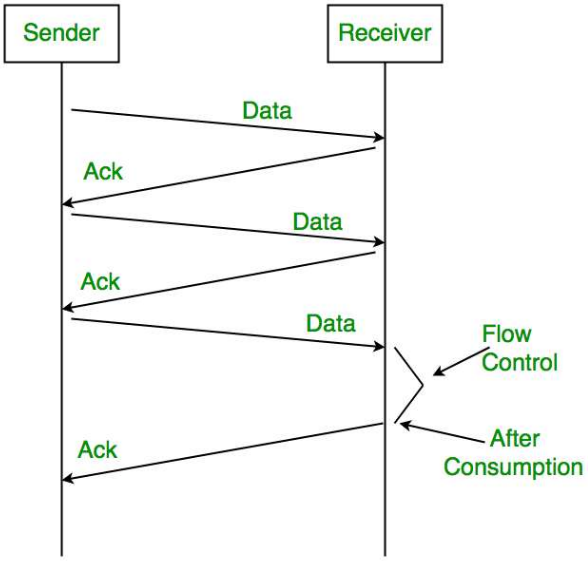
Simple Stop and Wait

At Sender

- Rule 1: Send one data packet at a time.
- Rule 2: Send the next packet only after receiving acknowledgment for the previous.

At Receiver

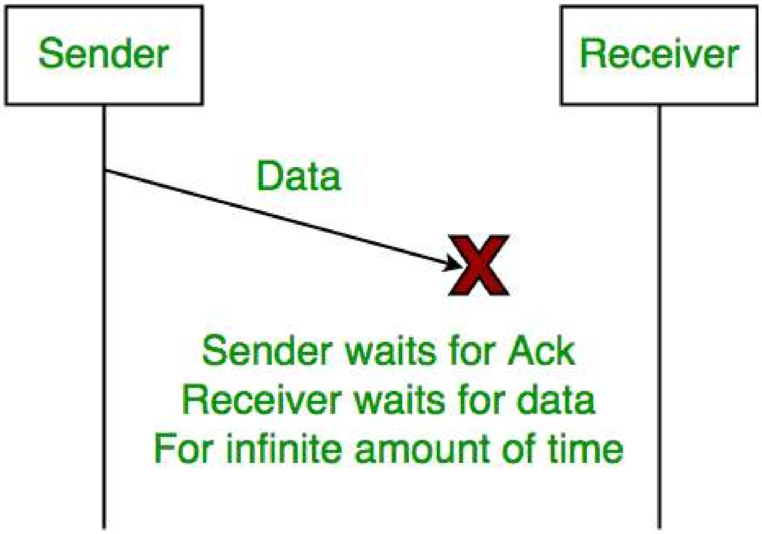
- Rule 1: Send acknowledgement after receiving and consuming a data packet.
- Rule 2: After consuming packet acknowledgement need to be sent (Flow Control)


Sender
Receiver
Data
Ack
Data
Ack
Data
Flow Control
After Consumption
Ack

Problems Associated with Stop and Wait

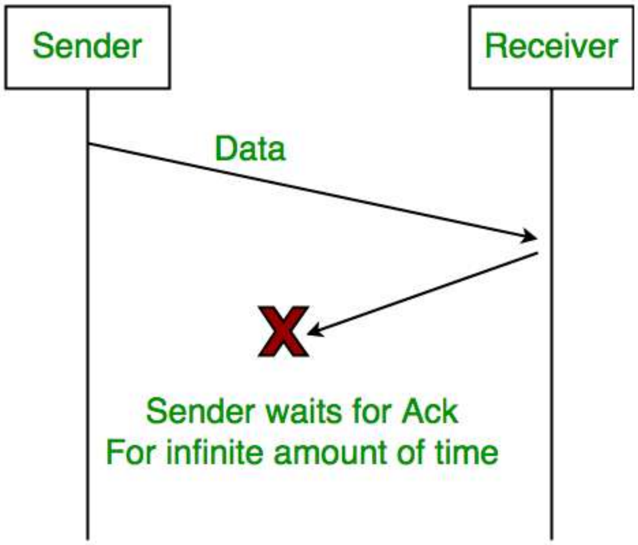
1. Lost Data

Assume the sender transmits the data packet and it is lost. The receiver has been waiting for the data for a long time. Because the data is not received by the receiver, it does not transmit an acknowledgment. The sender does not receive an acknowledgment, it will not send the next packet. This problem is caused by a loss of data.


Sender
Receiver
Data
Sender waits for Ack
Receiver waits for data
For infinite amount of time

2. Lost Acknowledgement

Assume the sender sends the data, which is also received by the receiver. The receiver sends an acknowledgment after receiving the packet. In this situation, the acknowledgment is lost in the network. The sender does not send the next data packet because it does not receive acknowledgement, under the stop and wait protocol, the next packet cannot be transmitted until the preceding packet's acknowledgment is received.

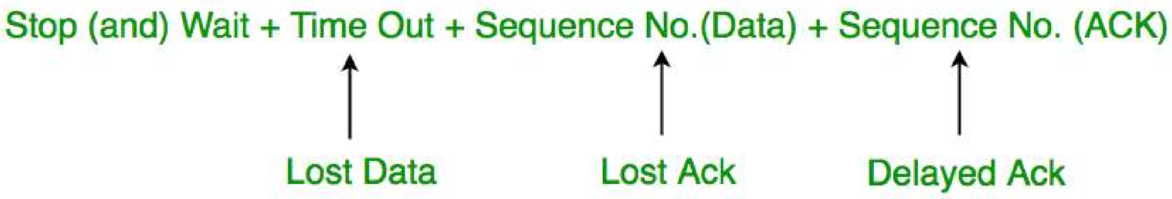


3. Delayed Acknowledgement/Data

Assume the sender sends the data, which is also received by the receiver. The receiver then transmits the acknowledgment, which is received after the sender's timeout period. After a timeout on the sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

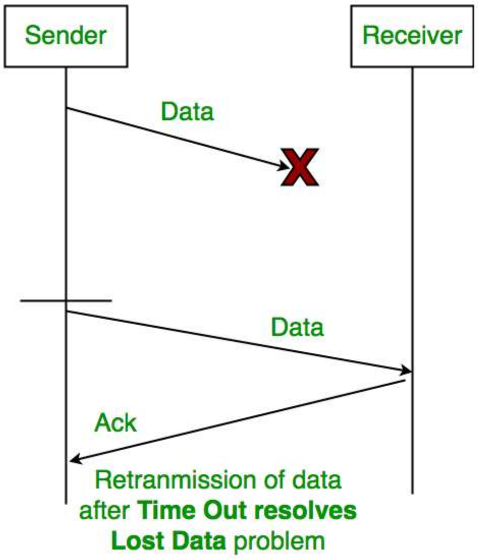
Stop and Wait for ARQ (Automatic Repeat Request)

The above 3 problems are resolved by Stop and Wait for ARQ (Automatic Repeat Request) that does both error control and flow control.


Stop (and) Wait + Time Out + Sequence No.(Data) + Sequence No. (ACK)
Lost Data
Lost Ack
Delayed Ack

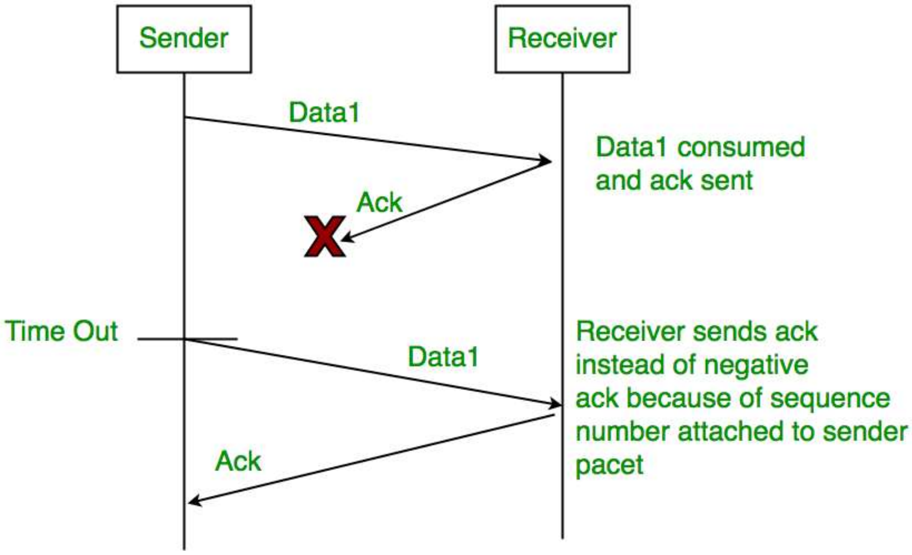
1. Time Out

Timeout refers to the duration for which the sender waits for an acknowledgment (ACK) from the receiver after transmitting a data packet. If the sender does not receive an ACK within this timeout period, it assumes that the frame was lost or corrupted and retransmits the frame.


Sender
Receiver
Data
Data
Ack
Retranmission of data
after Time Out resolves
Lost Data problem

2. Sequence Number (Data)

In Stop-and-Wait ARQ, the sender assigns sequence numbers to each data frame it sends. This allows the receiver to identify and acknowledge each frame individually, ensuring reliable delivery of data packets. After sending a frame, the sender waits for an acknowledgment before sending the next frame.


Sender
Receiver
Data1
Data1 consumed and ack sent
Ack
Time Out
Data1
Receiver sends ack instead of negative ack because of sequence number attached to sender pacet
Ack

3. Sequence Number(Acknowledgement)

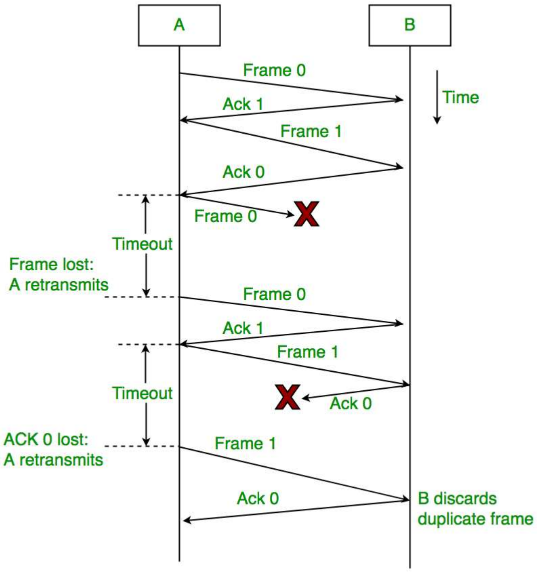
Similarly, sequence numbers are also used in acknowledgments (ACKs) sent by the receiver to acknowledge received data frames. When the

Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw

sender, indicating the sequence number of the next expected frame. The sender uses this ACK to determine whether the transmission was successful and whether it can proceed to send the next frame.

Working of Stop and Wait for ARQ

- Sender A sends a data frame or packet with sequence number 0.
- Receiver B, after receiving the data frame, sends an acknowledgement with sequence number 1 (the sequence number of the next expected data frame or packet)
  There is only a one-bit sequence number that implies that both sender and receiver have a buffer for one frame or packet only.


A
B
Frame 0
Time
Ack 1
Frame 1
Ack 0
Frame 0
Timeout
Frame lost:
A retransmits
Frame 0
Ack 1
Frame 1
Timeout
Ack 0
ACK 0 lost:
A retransmits
Frame 1
Ack 0
B discards
duplicate frame

Constraints in Stop and Wait ARQ

Stop and Wait ARQ has very less efficiency , it can be improved by increasing the window size. Also , for better efficiency , Go back N and Selective Repeat Protocols are used. The Stop and Wait ARQ solves the main three problems but may cause big performance issues as the sender always waits for acknowledgement even if it has the next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country through a high-speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence number. We will be discussing these protocols in the next articles. So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections but performs badly for distant connections like satellite connections.

Advantages of Stop and Wait ARQ

- **Simple Implementation:** Stop and Wait ARQ is a simple protocol that is easy to implement in both hardware and software. It does not require complex algorithms or hardware components, making it an inexpensive and efficient option.
- **Error Detection:** Stop and Wait ARQ detects errors in the transmitted data by using checksums or cyclic redundancy checks (CRC). If an error

is detected, the receiver sends a negative acknowledgment (NAK) to the sender, indicating that the data needs to be retransmitted.

- **Reliable:** Stop and Wait ARQ ensures that the data is transmitted reliably and in order. The receiver cannot move on to the next data packet until it receives the current one. This ensures that the data is received in the correct order and eliminates the possibility of data corruption.
- **Flow Control:** Stop and Wait ARQ can be used for flow control, where the receiver can control the rate at which the sender transmits data. This is useful in situations where the receiver has limited buffer space or processing power.
- **Backward Compatibility:** Stop and Wait ARQ is compatible with many existing systems and protocols, making it a popular choice for communication over unreliable channels.

Disadvantages of Stop and Wait ARQ

- **Low Efficiency:** Stop and Wait ARQ has low efficiency as it requires the sender to wait for an acknowledgment from the receiver before sending the next data packet. This results in a low data transmission rate, especially for large data sets.
- **High Latency:** Stop and Wait ARQ introduces additional latency in the transmission of data, as the sender must wait for an acknowledgment before sending the next packet. This can be a problem for real-time applications such as video streaming or online gaming.
- **Limited Bandwidth Utilization:** Stop and Wait ARQ does not utilize the available bandwidth efficiently, as the sender can transmit only one data packet at a time. This results in underutilization of the channel, which can be a problem in situations where the available bandwidth is limited.
- **Limited Error Recovery:** Stop and Wait ARQ has limited error recovery capabilities. If a data packet is lost or corrupted, the sender must retransmit the entire packet, which can be time-consuming and can result in further delays.

- **Vulnerable to Channel Noise:** Stop and Wait ARQ is vulnerable to channel noise, which can cause errors in the transmitted data. This can result in frequent retransmissions and can impact the overall efficiency of the protocol.

Question For Practice

Question: Suppose two hosts are connected by a point-to-point link and they are configured to use Stop and Wait protocol for reliable data transfer. Identify in which one of the following scenarios, the utilization of the link is the lowest. **[GATE CS/IT 2023]**

(A) Longer link length and lower transmission rate

(B) Longer link length and higher transmission rate

(C) Shorter link length and lower transmission rate

(D) Shorter link length and higher transmission rate

> ***Solution:*** *Correct option is (A)*
>
> ***Explanation-*** *Link utilization depends on **propagation delay** and **transmission rate**.*
>
> - ***Longer link length*** *increases **propagation delay**, reducing efficiency.*
> - ***Lower transmission rate*** *increases **waiting time**, further reducing efficiency.*
>
> *Thus, the **lowest utilization** occurs when the **link is long and the transmission rate is low**.*

Conclusion

From the above discussion we can conclude that the Stop and Wait ARQ is useful for point-to-point delivery and offers connection-oriented transmission along with flow and error control. It is mainly used in the transport layer and is reliable.

Sliding Window Protocol | Set 1 (Sender Side)

Last Updated : 25 Jul, 2024

Reliable data transmission is critical in computer networking, particularly across long distances or in networks that have high latency. The Sliding Window Protocol is a critical component in obtaining this reliability. It is part of the OSI model's Data Link Layer and is used in several protocols, including TCP. Sliding Window protocol handles efficiency issues by sending more than one packet at a time with a larger sequence number. The idea is the same as pipelining in architecture. In this article, we will discuss about Sliding Window Protocol.

What is Sliding Window Protocol?

The Sliding Window Protocol is a key computer networking technique for controlling the flow of data between two devices. It guarantees that data is sent consistently and effectively, allowing many packets to be sent before requiring an acknowledgment for the first, maximizing the use of available bandwidth.

Terminologies Related to Sliding Window Protocol

Transmission Delay (Tt) - Time to transmit the packet from the host to the outgoing link. If B is the Bandwidth of the link and D is the Data Size to transmit

```
Tt = D/B
```

Propagation Delay (Tp) - It is the time taken by the first bit transferred by the host onto the outgoing link to reach the destination. It depends on the distance d and the wave propagation speed s (depends on the characteristics of the medium).

```
   Tp = d/s
```

Efficiency - It is defined as the ratio of total useful time to the total cycle time of a packet. For stop and wait protocol,

```
 Total time(TT) = Tt(data) + Tp(data) +
                    Tt(acknowledgement) + Tp(acknowledgement)
                = Tt(data) + Tp(data) + Tp(acknowledgement)
           =   Tt + 2*Tp
```

Since acknowledgements are very less in size, their transmission delay can be neglected.

```
 Efficiency = Useful Time / Total Cycle Time
            = Tt/(Tt + 2*Tp) (For Stop and Wait)
            = 1/(1+2a)  [ Using a = Tp/Tt ]
```

Effective Bandwidth(EB) or Throughput - Number of bits sent per second.

```
 EB = Data Size(D) / Total Cycle time(Tt + 2*Tp)
 Multiplying and dividing by Bandwidth (B),
        =  (1/(1+2a)) * B   [ Using a = Tp/Tt ]
        =  Efficiency * Bandwidth
```

Capacity of link - If a channel is Full Duplex, then bits can be transferred in both the directions and without any collisions. Number of bits a channel/Link can hold at maximum is its capacity.

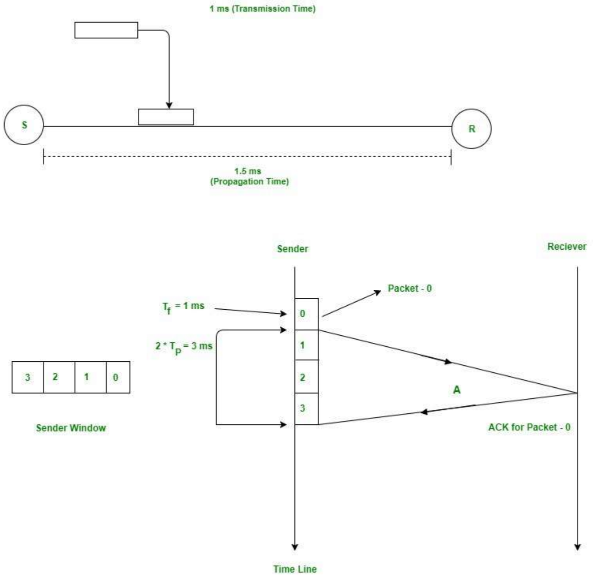
```
  Capacity = Bandwidth(B) * Propagation(Tp)

  For Full Duplex channels,
  Capacity = 2*Bandwidth(B) * Propagation(Tp)
```

Concept of Pipelining

In Stop and Wait protocol, only 1 packet is transmitted onto the link and then sender waits for acknowledgement from the receiver. The problem in this setup is that efficiency is very less as we are not filling the channel with more packets after 1st packet has been put onto the link. Within the total cycle time of Tt + 2*Tp units, we will now calculate the maximum number of packets that sender can transmit on the link before getting an acknowledgement.

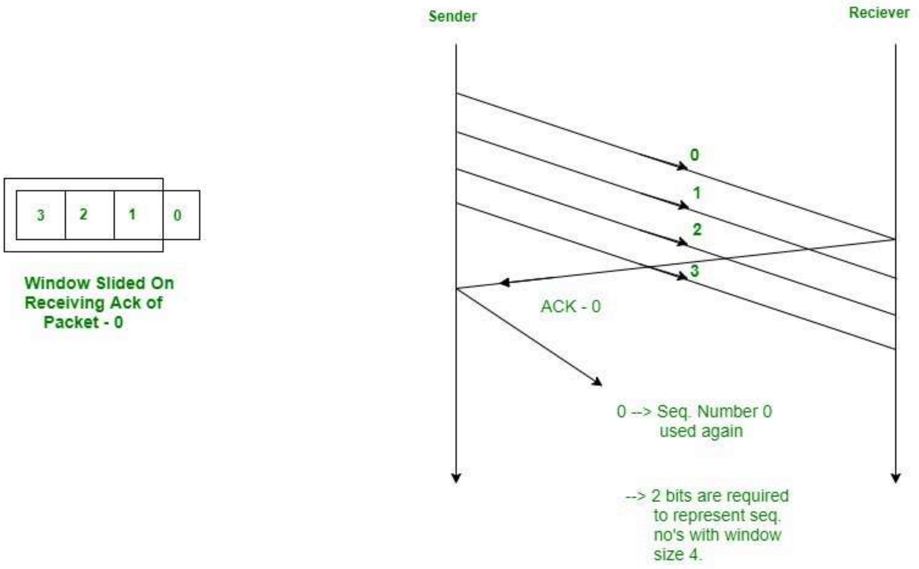
```
In Tt units ----> 1 packet is Transmitted.
In 1 units  ----> 1/Tt packet can be Transmitted.
In  Tt + 2*Tp units ----->  (Tt + 2*Tp)/Tt
                            packets can be Transmitted
               ------>  1 + 2a  [Using a = Tp/Tt]
```

Maximum packets That can be Transmitted in total cycle time = 1+2*a Let me explain now with the help of an example. Consider Tt = 1ms, Tp = 1.5ms. In the picture given below, after sender has transmitted packet 0, it will immediately transmit packets 1, 2, 3. Acknowledgement for 0 will arrive after 2*1.5 = 3ms. In Stop and Wait, in time 1 + 2*1.5 = 4ms, we were transferring one packet only. Here we keep a **window of packets that we have transmitted but not yet acknowledged**.



After we have received the Ack for packet 0, window slides and the next packet can be assigned sequence number 0. We reuse the sequence

minimum as shown in the diagram given below.


Sender
Reciever
3
2
1
0
Window Slided On Receiving Ack of Packet - 0
0
1
2
3
ACK - 0
0 --> Seq. Number 0 used again
--> 2 bits are required to represent seq. no's with window size 4.

Minimum Number of Bits For Sender Window (Very Important For GATE)

As we have seen above,

```
Maximum window size = 1 + 2*a     where a = Tp/Tt

Minimum sequence numbers required = 1 + 2*a.
```

All the packets in the current window will be given a sequence number. Number of bits required to represent the sender window = ceil(log2(1+2*a)). But sometimes number of bits in the protocol headers is pre-defined. Size of sequence number field in header will also determine the maximum number of packets that we can send in total cycle time. If N is the size of sequence number field in the header in bits, then we can have 2^N sequence numbers. Window Size ws = min(1+2*a, 2^N) If you want to calculate minimum bits required to represent sequence numbers/sender window, it will be **ceil(log2(ws))**. In this article, we have discussed sending window only. For receiving window, there are 2 protocols namely **Go Back N** and **Selective Repeat** which are used to implement pipelining practically. We will be discussing receiving window in set 2.

Types of Sliding Window Protocol

There are two types of Sliding Window Protocol which include Go-Back-N ARQ and Selective Repeat ARQ:

1. Go-Back-N ARQ

Go-Back-N ARQ allows sending more than one frame before getting the first frame's acknowledgment. It is also known as sliding window protocol since it makes use of the sliding window notion. There is a limit to the amount of frames that can be sent, and they are numbered consecutively. All frames beginning with that frame are retransmitted if the acknowledgment is not received in a timely manner. For more detail visit the page Go-Back-N ARQ.

2. Selective Repeat ARQ

Additionally, this protocol allows additional frames to be sent before the first frame's acknowledgment is received. But in this case, the excellent frames are received and buffered, and only the incorrect or lost frames are retransmitted. Check the detailed explanation of Selective Repeat ARQ.

Advantages of Sliding Window Protocol

- **Efficiency:** The sliding window protocol is an efficient method of transmitting data across a network because it allows multiple packets to be transmitted at the same time. This increases the overall throughput of the network.
- **Reliable:** The protocol ensures reliable delivery of data, by requiring the receiver to acknowledge receipt of each packet before the next packet can be transmitted. This helps to avoid data loss or corruption during transmission.
- **Flexibility:** The sliding window protocol is a flexible technique that can be used with different types of network protocols and topologies, including wireless networks, Ethernet, and IP networks.
- **Congestion Control:** The sliding window protocol can also help control network congestion by adjusting the size of the window based on the

network conditions.

Disadvantages of Sliding Window Protocol

- **Complexity:** The sliding window protocol can be complex to implement and can require a lot of memory and processing power to operate efficiently.
- **Delay:** The protocol can introduce a delay in the transmission of data, as each packet must be acknowledged before the next packet can be transmitted. This delay can increase the overall latency of the network.
- **Limited Bandwidth Utilization:** The sliding window protocol may not be able to utilize the full available bandwidth of the network, particularly in high-speed networks, due to the overhead of the protocol.
- **Window Size Limitations:** The maximum size of the sliding window can be limited by the size of the receiver's buffer or the available network resources, which can affect the overall performance of the protocol.

Difference between the Go-Back-N ARQ and Selective Repeat ARQ

Go-Back-N Protocol	Selective Repeat Protocol
In Go-Back-N Protocol, if the sent frame are find suspected then all the frames are re-transmitted from the lost packet to the last packet transmitted.	In selective Repeat protocol, only those frames are re-transmitted which are found suspected.
Sender window size of Go-Back-N Protocol is N.	Sender window size of selective Repeat protocol is also N.

Go-Back-N Protocol	Selective Repeat Protocol
Receiver window size of Go-Back-N Protocol is 1.	Receiver window size of selective Repeat protocol is N.
Go-Back-N Protocol is less complex.	Selective Repeat protocol is more complex.
In Go-Back-N Protocol, neither sender nor at receiver need sorting.	In selective Repeat protocol, receiver side needs sorting to sort the frames.
In Go-Back-N Protocol, type of Acknowledgement is cumulative.	In selective Repeat protocol, type of Acknowledgement is individual.
In Go-Back-N Protocol, Out-of-Order packets are NOT Accepted (discarded) and the entire window is re-transmitted.	In selective Repeat protocol, Out-of-Order packets are Accepted.
In Go-Back-N Protocol, if Receives a corrupt packet, then also, the entire window is re-transmitted.	In selective Repeat protocol, if Receives a corrupt packet, it immediately sends a negative acknowledgement and hence only the selective packet is retransmitted.
Efficiency of Go-Back-N Protocol is `N/(1+2*a)`	Efficiency of selective Repeat protocol is also `N/(1+2*a)`

Conclusion

The Sliding Window Protocol is a crucial technique for assuring reliable and efficient data delivery in computer networks. Allowing many packets to be delivered before demanding acknowledgments and maximizes bandwidth use and minimizes delays. This protocol, which is implemented in forms such as Go-Back-N ARQ and Selective Repeat ARQ, maintains a balance between efficiency and reliability, despite the increased complexity and potential transmission latency.

Comment More info Advertise with us

Next Article

What is MAC Address?

Similar Reads

1. Sliding Window Protocol | Set 3 (Selective Repeat)
2. Sliding Window Protocol - Go Back N (GBN)
3. Birman Schiper Stephenson Protocol
4. Schiper Eggli Sandoz Protocol
5. Real Time Transport Protocol (RTP)
6. Routing Protocol Code
7. What is TCP (Transmission Control Protocol)?
8. What is Signaling Connection Control Part (SCCP)?
9. File transfer protocol server configuration using cisco packet tracer
10. Transport Layer Protocols

Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Registered Address:
K 061, Tower K, Gulshan Vivante
Apartment, Sector 137, Noida, Gautam
Buddh Nagar, Uttar Pradesh, 201305

IPv4 Datagram Header

Last Updated : 04 Feb, 2025

IP stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983. IP version four addresses are 32-bit integers which will be expressed in decimal notation. In this article, we will discuss about IPv4 datagram header.

IPv4 is a connectionless protocol used for packet-switched networks. Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type. IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B, and C have a different bit length for addressing the network host. Class D addresses are reserved for multicasting, while class E addresses are reserved for military purposes. IPv4 uses 32-bit (4-byte) addressing, which gives 2^{32} addresses. IPv4 addresses are written in the dot-decimal notation, which comprises four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.

- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask)

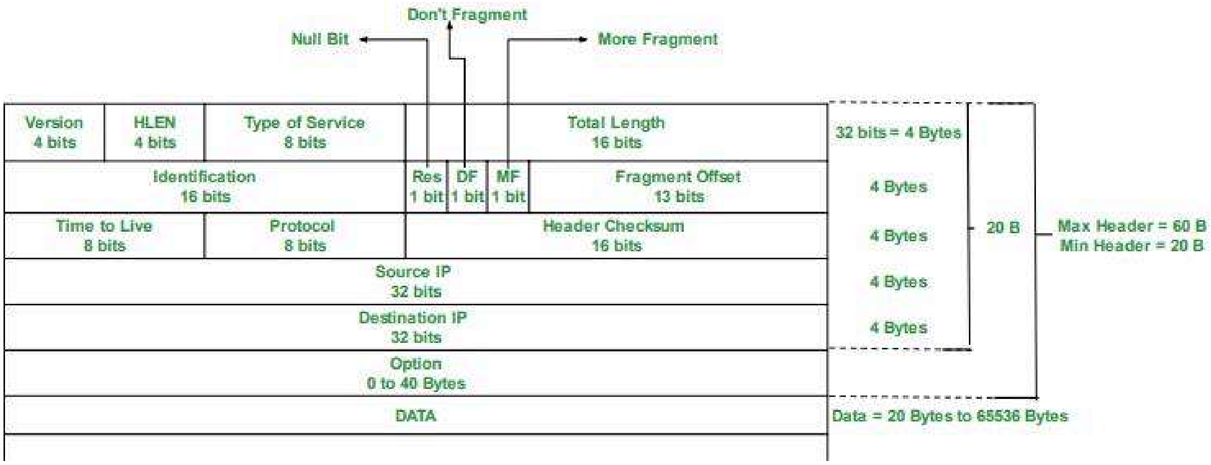
address.

- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

IPv4 Datagram Header

- **VERSION***:* Version of the IP protocol (4 bits), which is 4 for IPv4
- **HLEN:** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.
- **Type of service:** Low Delay, High Throughput, Reliability (8 bits)
- **Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.
- **Identification***:* Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)
- **Flags***:* 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
- **Fragment Offset:** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.
- **Time to live***:* Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.
- **Protocol:** Name of the protocol to which the data is to be passed (8 bits)
- **Header Checksum***:* 16 bits header checksum for checking errors in the datagram header
- **Source IP address***:* 32 bits IP address of the sender

- **Destination IP address*:*** 32 bits IP address of the receiver
- **Option:** Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.


Don't Fragment
Null Bit
More Fragment
Version 4 bits
HLEN 4 bits
Type of Service 8 bits
Total Length 16 bits
Identification 16 bits
Res 1 bit
DF 1 bit
MF 1 bit
Fragment Offset 13 bits
Time to Live 8 bits
Protocol 8 bits
Header Checksum 16 bits
Source IP 32 bits
Destination IP 32 bits
Option 0 to 40 Bytes
DATA
32 bits = 4 Bytes
4 Bytes
4 Bytes
4 Bytes
4 Bytes
20 B
Max Header = 60 B
Min Header = 20 B
Data = 20 Bytes to 65536 Bytes

IPv4 Datagram Header

Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

Comment More info Advertise with us

Next Article

Difference between Unicast, Broadcast and Multicast in Computer Network

Similar Reads

1. HTTP headers | Early-Data
2. HTTP headers | Date
3. IPv6 Fragmentation Header
4. HTTP headers | DNT
5. IPv4 Datagram Fragmentation and Delays
6. Framing in Data Link Layer
7. HTTP headers | Digest
8. Datagram Delivery Protocol (DDP)

Introduction of Classful IP Addressing

Last Updated : 14 Jan, 2025

An **IP address** is an address that has information about how to reach a specific host, especially outside the LAN. An IP address is a 32-bit unique address having an address space of 2^{32}.

Classful IP addressing is a way of organizing and managing IP addresses, which are used to identify devices on a network. Think of IP addresses like street addresses for houses; each device on a network needs its unique address to communicate with other devices. In this article, we will discuss Classful IP addresses, and their types in detail.

Classful IP Addressing

Classful IP addressing is an obsolete method for allocating IP addresses and dividing the available IP address space across networks. It was used from 1981 to 1993 until the introduction of CIDR (Based on Prefixes rather than classes). Classful method categorizes IP addresses into five classes (A, B, C, D, and E), each defined by the first few bits of the address and serving specific ranges of purposes. The functionality of classful networking also extended to ease of configuration. Network administrators could set up networks with default subnet masks without the need for detailed subnetting strategies, which was particularly beneficial in less complex networking environments.

IPV4 Address

An **IPv4 address** is a unique number assigned to every device that connects to the internet or a computer network. It's like a home address for your computer, smartphone, or any other device, allowing it to communicate with other devices.

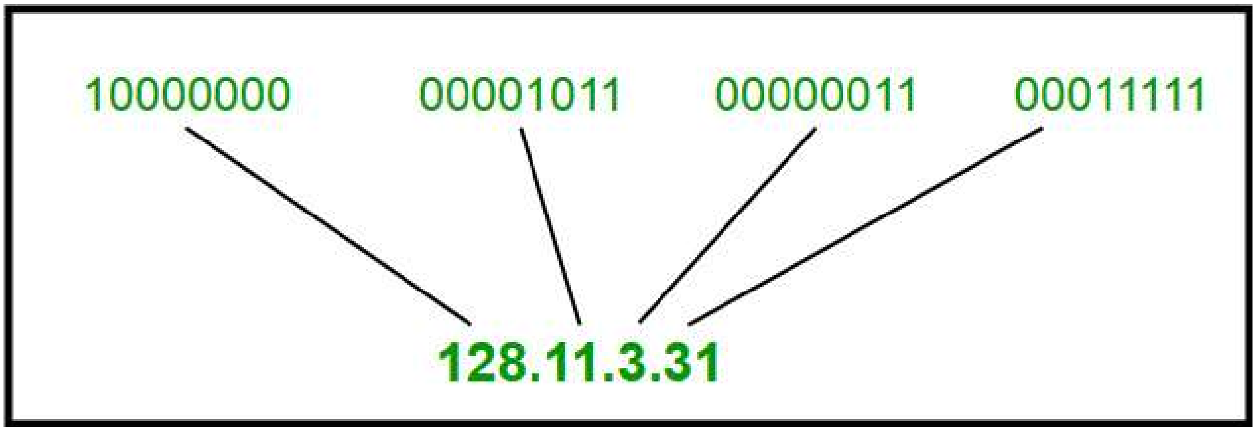
- **Format**: An IPv4 address is written as four numbers separated by periods, like this: 192.168.1.1. Each number can range from 0 to 255.
- The IPv4 address is divided into two parts: **NID (Network ID)** = 8bit, and **HID (Host ID)** = 24bit. So there are 2^8 which is 256 total networks created and 2^{24} which is 16M Host per network.
- **Purpose**: The main purpose of an IPv4 address is to identify devices on a network and ensure that data sent from one device reaches the correct destination.
- **Example**: When you type a website address into your browser, your device uses the IPv4 address to find and connect to the server where the website is hosted.

There are two notations in which the IP address is written, dotted decimal and hexadecimal notation.

Dotted Decimal Notation

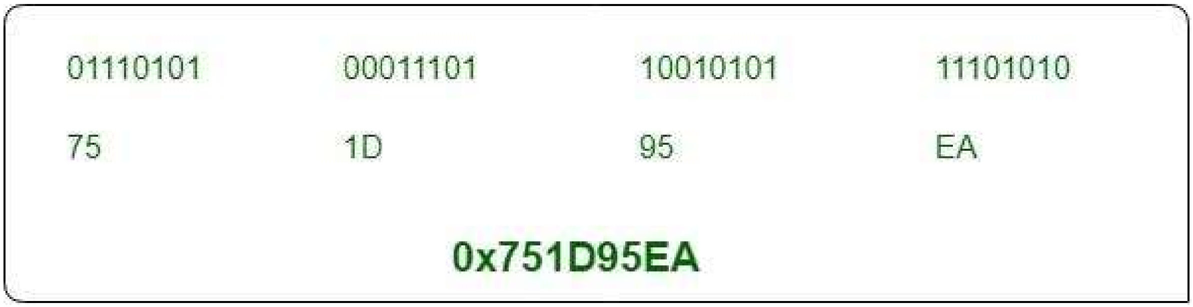
Some points to be noted about dotted decimal notation:

- The value of any segment (byte) is between 0 and 255 (both included).
- No zeroes preceding the value in any segment (054 is wrong, 54 is correct).



Dotted Decimal Notation

Hexadecimal Notation



01110101	00011101	10010101	11101010
75	1D	95	EA

0x751D95EA

Need For Classful Addressing

- Classful addressing provided a straightforward method to allocate and manage IP addresses based on fixed classes, simplifying the administrative burden associated with IP address distribution.

- Network equipment of the time, such as routers, could be more easily programmed to handle a limited number of fixed classes, speeding up the routing process because the class of an address could be quickly identified from its first few bits.

- While it did have limitations, classful addressing allowed for scaling of networks within the bounds of each class size. Larger networks could use a Class A or B address, and smaller networks could operate efficiently within a Class C subnet.

- By standardizing address ranges, classful addressing facilitated the implementation of uniform network protocols, which was important for the interoperability of network devices across different networks and platforms.

- Classful addressing was a cost-effective solution that supported the early expansion of the Internet by avoiding the need for complex subnetting schemes that require additional computing resources and more sophisticated network management tools.

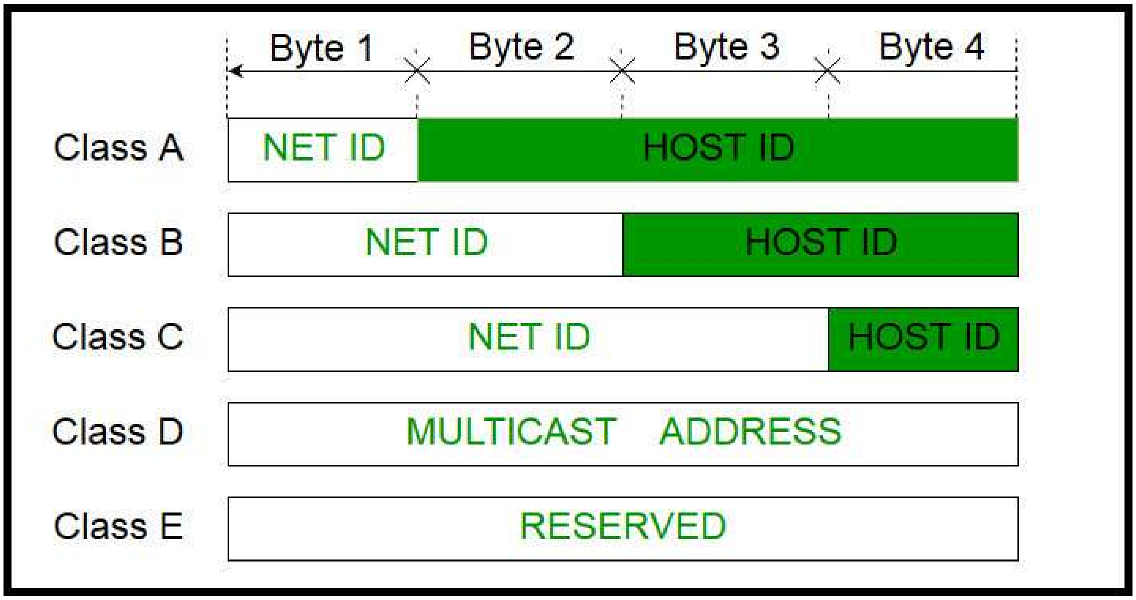
Classes of IP Addressing

The 32-bit IP address is divided into five sub-classes. These are given below:

- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determines the classes of the IP address.

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns an IP address to each device that is connected to its network.

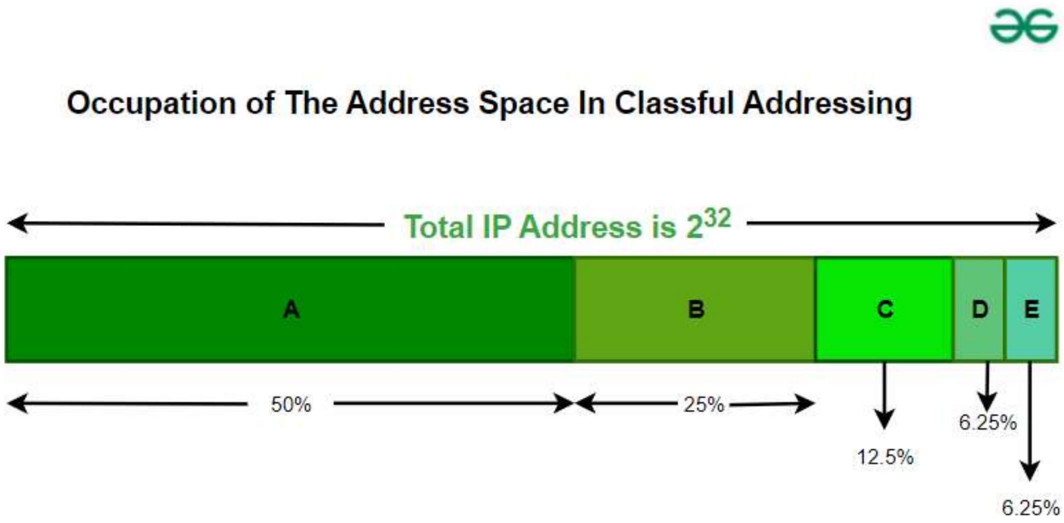

Byte 1
Byte 2
Byte 3
Byte 4
Class A
NET ID
HOST ID
Class B
NET ID
HOST ID
Class C
NET ID
HOST ID
Class D
MULTICAST ADDRESS
Class E
RESERVED

Classful Addressing

Note:

- IP addresses are globally managed by Internet Assigned Numbers Authority (IANA) and Regional Internet Registries (RIR).
- While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because

the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.



Occupation of The Address Space In Classful Addressing

Class A

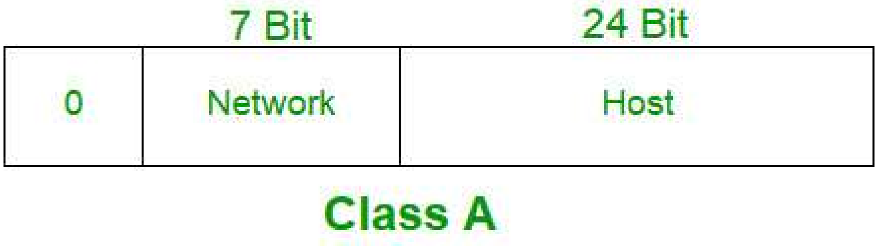
IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher-order bit of the first octet in class A is always set to 0. The remaining 7 bits in the first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for Class A is 255.x.x.x. Therefore, class A has a total of:

- $2^{24} - 2 = 16,777,214$ host ID

IP addresses belonging to class A ranges from 0.0.0.0 - 127.255.255.255.



Class A

Class B

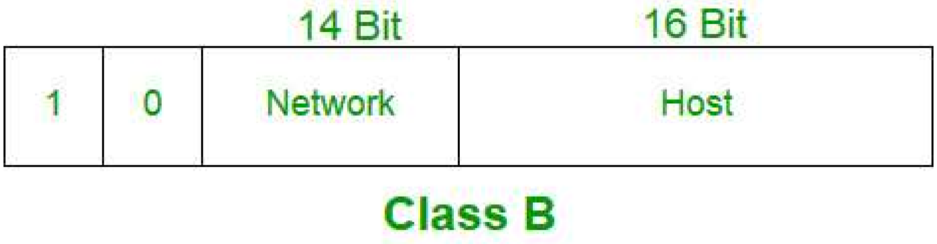
IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher-order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet mask for class B is 255.255.x.x. Class B has a total of:

- 2^{14} = 16384 network address
- 2^{16} - 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.0.0 – 191.255.255.255.



Class B

Class C

IP addresses belonging to class C are assigned to small-sized networks.

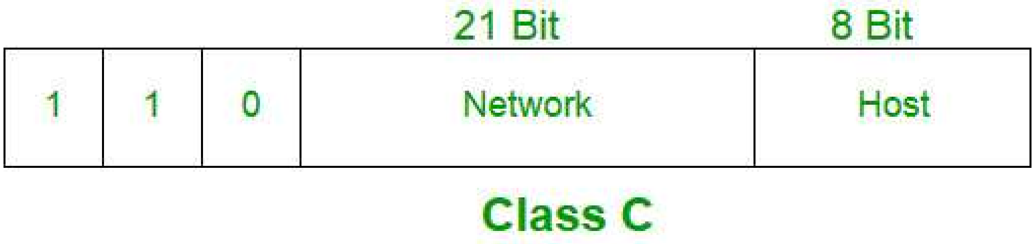
- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher-order bits of the first octet of IP addresses of class C is always set to 110. The remaining 21 bits are used to determine the network ID.

The 8 bits of host ID are used to determine the host in any network. The default subnet mask for class C is 255.255.255.x. Class C has a total of:

- 2^{21} = 2097152 network address
- 2^{8} – 2 = 254 host address

IP addresses belonging to class C range from 192.0.0.0 – 223.255.255.255.

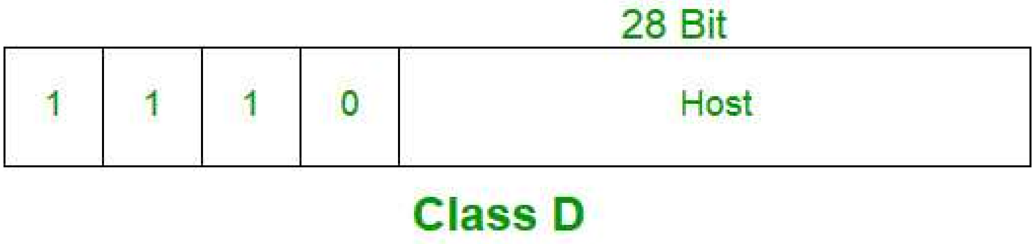


Class C

Class D

IP address belonging to class D is reserved for multi-casting. The higher-order bits of the first octet of IP addresses belonging to class D is always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.

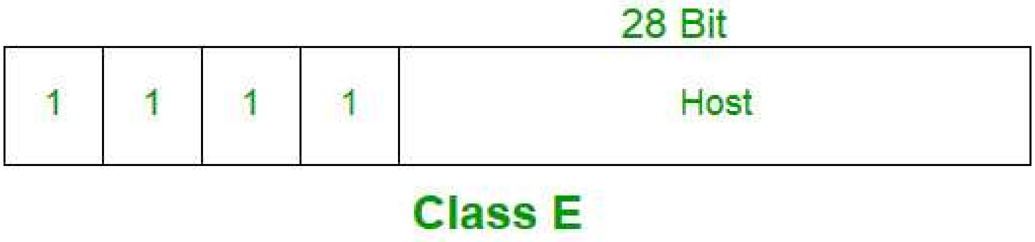


Class D

Class E

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 –

255.255.255.255. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.



Class E

Range of Special IP Addresses

```
169.254.0.0 – 169.254.0.16 : Link-local addresses
127.0.0.0 – 127.255.255.255 : Loop-back addresses
0.0.0.0 – 0.0.0.8: used to communicate within the current network.
```

Rules for Assigning Host ID

Host IDs are used to identify a host within a network. The host ID is assigned based on the following rules:

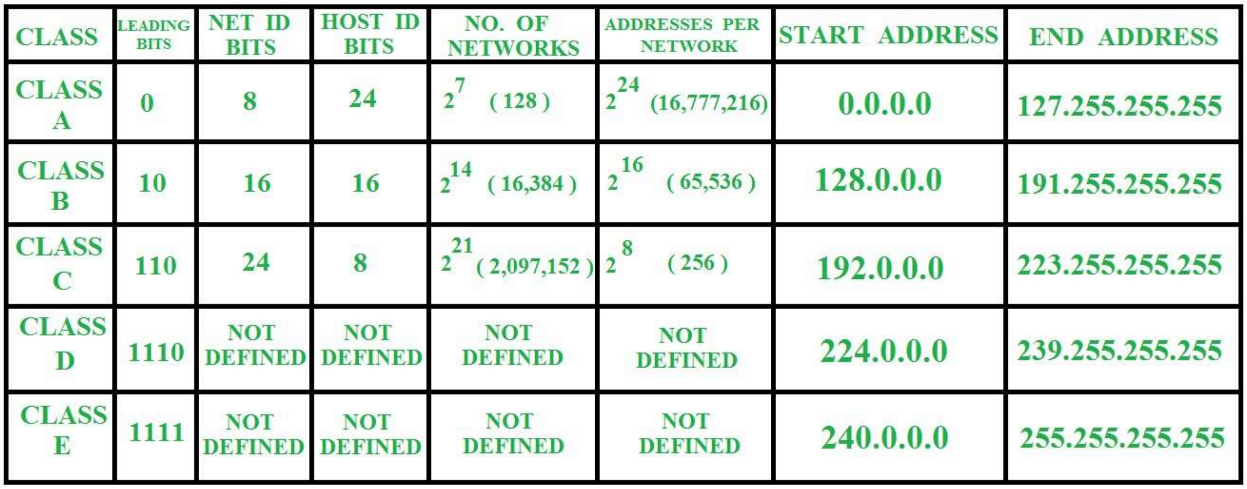
- Within any network, the host ID must be unique to that network.
- A host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for Assigning Network ID

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to the class A address and is reserved for internal loopback functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Structure of Classful Addressing



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

In the above table No. of networks for class A should be 127. (Network ID with all 0 s is not considered)

Problems With Classful Addressing

The problem with this classful addressing method is that millions of class A addresses are wasted, many of the class B addresses are wasted, whereas, the number of addresses available in class C is so small that it cannot cater to the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993. We will be discussing Classless addressing in the next post.

- The network ID is 24 bits long.
- The host ID is 8 bits long.
- 2^{21} = 2097152 network address
- 2^8 - 2 = 254 host address
- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

- The network ID cannot start with 127 because 127 belongs to the class A address and is reserved for internal loopback functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Classful and Classless Addressing

Here is the main difference between Classful and Classless Addressing:

Parameter	Classful Addressing	Classless Addressing
Basics	In Classful addressing IP addresses are allocated according to the classes- A to E.	Classless addressing came to replace the classful addressing and to handle the issue of rapid exhaustion of IP addresses.
Practical	It is less practical.	It is more practical.
Network ID and Host ID	The changes in the Network ID and Host ID depend on the class.	There is no such restriction of class in classless addressing.
VLSM	It does not support the Variable Length Subnet Mask (VLSM).	It supports the Variable Length Subnet Mask (VLSM).
Bandwidth	Classful addressing requires more bandwidth. As a result, it becomes slower and more	It requires less bandwidth. Thus, fast and less expensive as

Parameter	Classful Addressing	Classless Addressing
	expensive as compared to classless addressing.	compared to classful addressing.
CIDR	It does not support Classless Inter-Domain Routing (CIDR).	It supports Classless Inter-Domain Routing (CIDR).
Updates	Regular or periodic updates	Triggered Updates
Troubleshooting and Problem detection	Troubleshooting and problem detection are easy than classless addressing because of the division of network, host and subnet parts in the address.	It is not as easy compared to classful addressing.
Division of Address	• Network • Host • Subnet	• Host • Subnet

Conclusion

Classful IP addressing, with its categorization into classes like A, B, and C, was a fundamental method in early networking. It organized IP addresses based on network size but faced limitations in flexibility and efficient use of address space. The development of CIDR addressed these issues by allowing more precise control over subnetting and optimizing address allocation.

Comment More info Advertise with us

Next Article

Types of Routing

Last Updated : 27 May, 2025

Routing is the process of determining paths through a network for sending data packets. It ensures that data moves effectively from source to destination, making the best use of network resources and ensuring

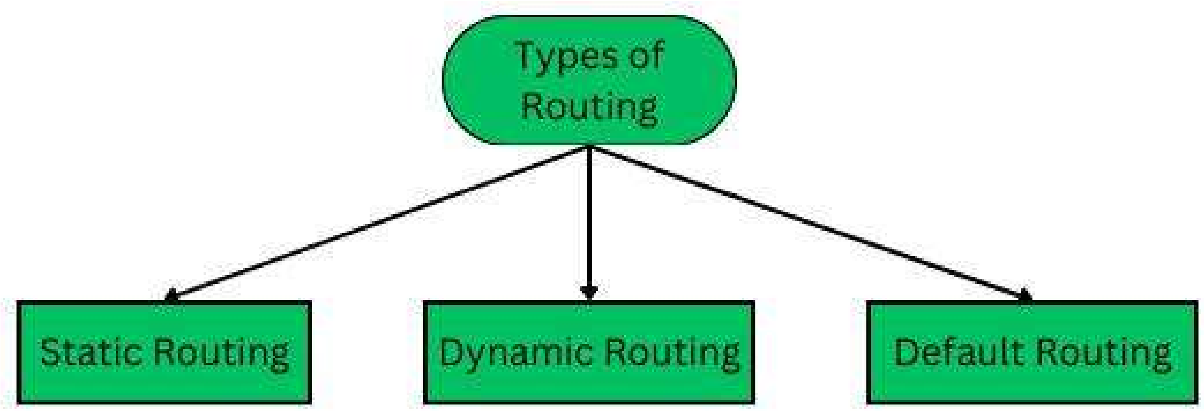
Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw

Routing is performed by layer 3 (or network layer) devices to deliver the packet by choosing an optimal path from one network to another. It is an autonomous process handled by the network devices to direct a data packet to its intended destination. The node here refers to a network device called Router.

Routing is essential for determining the optimal path for data packets across networks. Different routing techniques, such as static, dynamic, and hybrid, are used depending on the network. The **GATE CS Self-Paced Course** provides thorough coverage of routing algorithms, making it easier to grasp this critical networking concept

Types of Routing

Routing is typically of 3 types, each serving its purpose and offering different functionalities.



Types of Routing

1. Static Routing

Static routing is also called as “non-adaptive routing”. In this, routing configuration is done manually by the network administrator. Let’s say for example, we have 5 different routes to transmit data from one node to another, so the network administrator will have to manually enter the routing information by assessing all the routes.

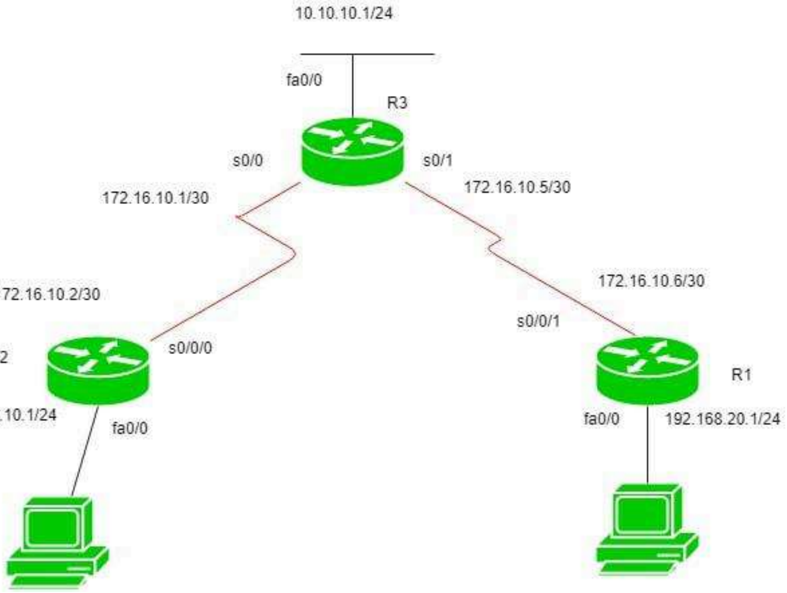
Advantages of Static Routing

- No routing overhead for the router CPU which means a cheaper router can be used to do routing.
- It adds security because only an only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantage of Static Routing

- For a large network, it is a hectic task for administrators to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Configuration of Static Routing


10.10.10.1/24
fa0/0
R3
s0/0
s0/1
172.16.10.1/30
172.16.10.5/30
172.16.10.6/30
172.16.10.2/30
s0/0/1
R2
s0/0/0
R1
192.168.10.1/24
fa0/0
fa0/0
192.168.20.1/24

R1 having IP address 172.16.10.6/30 on s0/0/1, 192.168.20.1/24 on fa0/0.
R2 having IP address 172.16.10.2/30 on s0/0/0, 192.168.10.1/24 on fa0/0.
R3 having IP address 172.16.10.5/30 on s0/1, 172.16.10.1/30 on s0/0, 10.10.10.1/24 on fa0/0.

Now because only static routes for router R3:

```
R3(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.2
R3(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.6
```

Here, provided the route for the 192.168.10.0 network where 192.168.10.0 is its network I'd and 172.16.10.2 and 172.16.10.6 are the next-hop address.
Now, configuring for R2:

```
R2(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.1
R2(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.1
R2(config)#ip route 172.16.10.0 255.255.255.0 172.16.10.1
```

Similarly for R1:

```
R1(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.5
R1(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.5
R1(config)#ip route 172.16.10.0 255.255.255.0 172.16.10.5
```

2. Default Routing

This is the method where the router is configured to send all packets toward a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing. It is generally used with stub routers. A stub router is a router that has only one route to reach all other networks.

Advantages of Default Routing

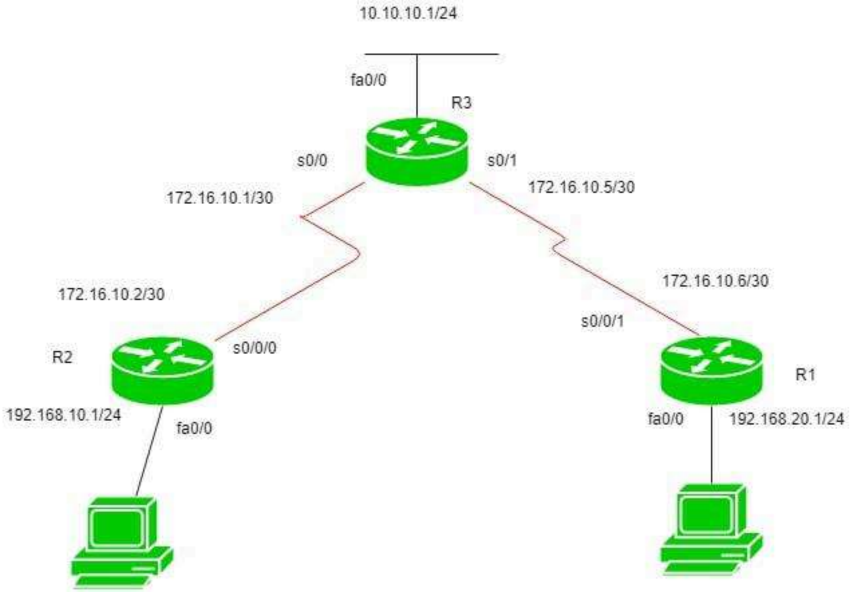
- Default routing provides a “last resort” route for packets that don’t match any specific route in the routing table. It ensures that packets are not dropped and can reach their intended destination.
- It simplifies network configuration by reducing the need for complex routing tables.
- Default routing improves network reliability and reduces packet loss.

Disadvantages of Default Routing

- Relying solely on default routes can lead to inefficient routing, as it doesn’t consider specific paths.
- Using default routes may introduce additional network latency.

Configuration of Default Routing

Using the same topology which we have used for static routing before.


10.10.10.1/24
fa0/0
R3
s0/0
s0/1
172.16.10.1/30
172.16.10.5/30
172.16.10.6/30
172.16.10.2/30
s0/0/1
R2
s0/0/0
R1
192.168.10.1/24
fa0/0
fa0/0
192.168.20.1/24

In this topology, R1 and R2 are stub routers so we can configure default routing for both these routers. Configuring default routing for R1:

> *R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.5*

Now configuring default routing for R2:

> *R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.1*

3. Dynamic Routing

Dynamic routing makes automatic adjustments of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach them. RIP and OSPF are the best examples of dynamic routing protocols. Automatic adjustments will be made to reach the network destination if one route goes down. A dynamic protocol has the following features:

- The routers should have the same dynamic protocol running in order to exchange routes.
- When a router finds a change in the topology then the router advertises it to all other routers.

Advantages of Dynamic Routing

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote networks.

Disadvantage of Dynamic Routing

- Consumes more bandwidth for communicating with other neighbors.
- Less secure than static routing.

Comment More info Advertise with us

Next Article

Difference between Static and Dynamic Routing

Similar Reads

1. What is Routing?
2. What is IP Routing?
3. Types of Network Topology
4. RPL (IPv6 Routing protocol)
5. Traffic Aware Routing
6. Routing Tables in Computer Network
7. Unicast Routing - Link State Routing
8. OSPF Area Types
9. Host Routes in CCNA
10. Types of APPN Nodes

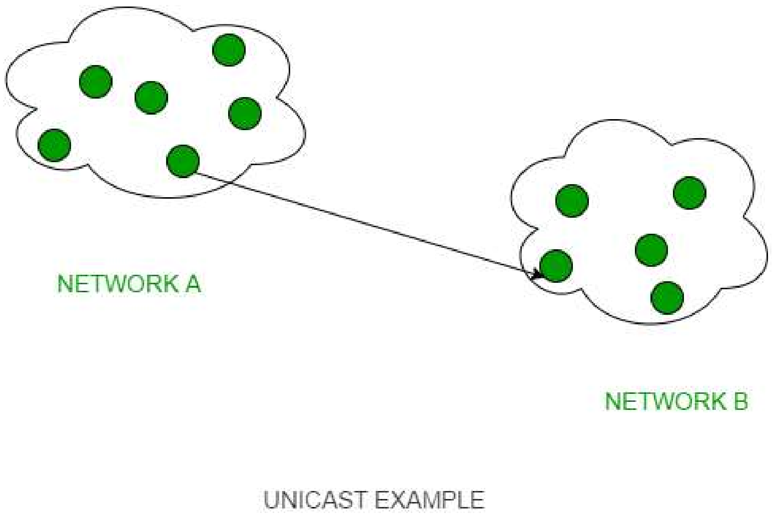
Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh

Unicast Routing - Link State Routing

Last Updated : 05 Feb, 2025

Unicast means the transmission from a single sender to a single receiver. It is a point-to-point communication between the sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCP (Transmission Control Protocol) is the most commonly used unicast protocol. It is a connection-oriented protocol that relies on acknowledgment from the receiver side.
- HTTP stands for HyperText Transfer Protocol. It is an object-oriented protocol for communication.



Unicast Routing

Major Protocols of Unicast Routing

1. **Distance Vector Routing:** Distance-Vector routers use a distributed algorithm to compute their routing tables.
2. **Link-State Routing:** Link-State routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.

3. **Path-Vector Routing:** It is a routing protocol that maintains the path that is updated dynamically.

Link State Routing

Link state routing is the second family of routing protocols. While distance-vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router i.e. the internet work. The three keys to understand the link state routing algorithm.

1. **Knowledge about the neighborhood** : Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
2. **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as flooding. Every router that receives the packet sends the copies to all the neighbors. Finally each and every router receives a copy of the same information.
3. **Information Sharing** : A router send the information to every other router only when the change occurs in the information.

Link state routing has two phase:

1. **Reliable Flooding: Initial state** - Each node knows the cost of its neighbors. Final state- Each node knows the entire graph.
2. **Route Calculation** : Each node uses Dijkstra' s algorithm on the graph to calculate the optimal routes to all nodes. The link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.

Features of Link State Routing Protocols

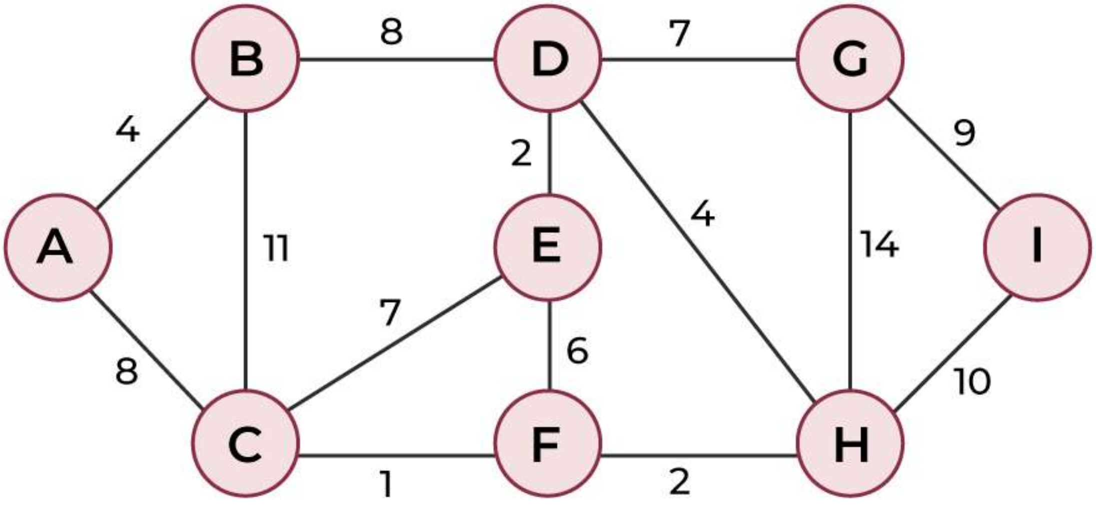
- **Link State Packet:** A small packet that contains routing information.
- **Link-State Database:** A collection of information gathered from the link-state packet.
- **Shortest Path First Algorithm (Dijkstra algorithm):** A calculation performed on the database results in the shortest path
- **Routing Table:** A list of known paths and interfaces.

Calculation of Shortest Path

To find the shortest path, each node needs to run the famous Dijkstra algorithm. Let us understand how can we find the shortest path using an example.

Note: We use a boolean array **sptSet[]** to represent the set of vertices included in SPT. If a value **sptSet[v]** is true, then vertex v is included in SPT, otherwise not. Array **dist[]** is used to store the shortest distance values of all vertices.

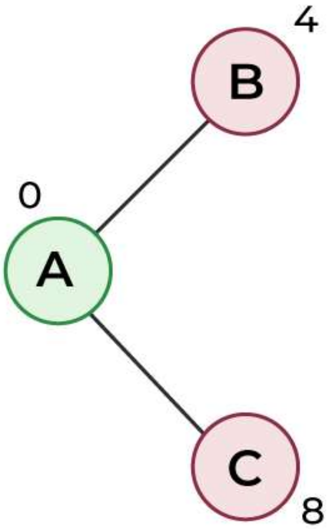
Consider the below graph and src = 0.



Shortest Path Calculation - Step 1

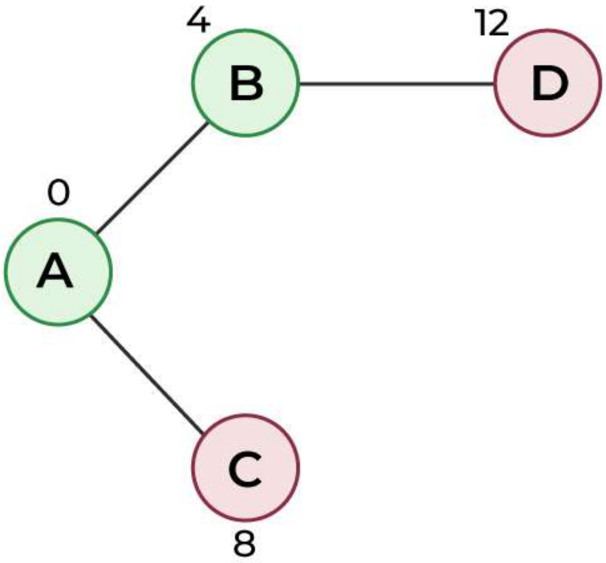
STEP 1: The set sptSet is initially empty and distances assigned to vertices are {0, INF, INF, INF, INF, INF, INF, INF} where INF indicates infinite. Now pick the vertex with a minimum distance value. The vertex 0 is picked and included in sptSet. So sptSet becomes {0}. After including 0 to sptSet, update the distance values of its adjacent vertices. Adjacent vertices of 0 are 1 and 7. The distance values of 1 and 7 are updated as 4 and 8.

The following subgraph shows vertices and their distance values. Vertices included in SPT are included in GREEN color.



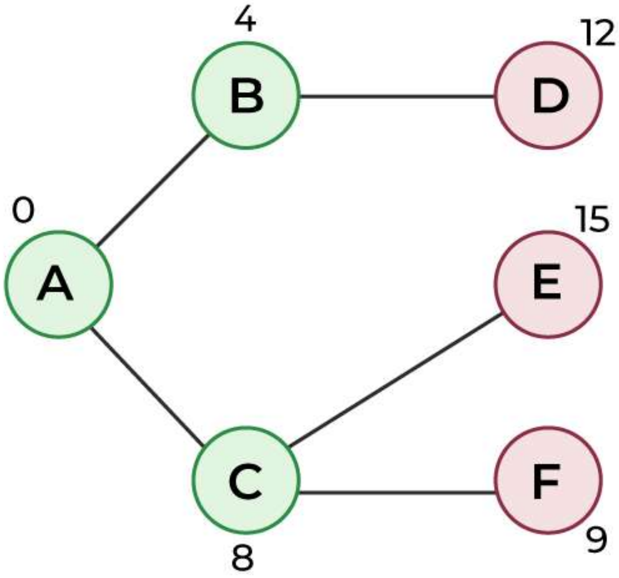
Shortest Path Calculation - Step 2

STEP 2: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). The vertex 1 is picked and added to sptSet. So sptSet now becomes {0, 1}. Update the distance values of adjacent vertices of 1. The distance value of vertex 2 becomes 12.



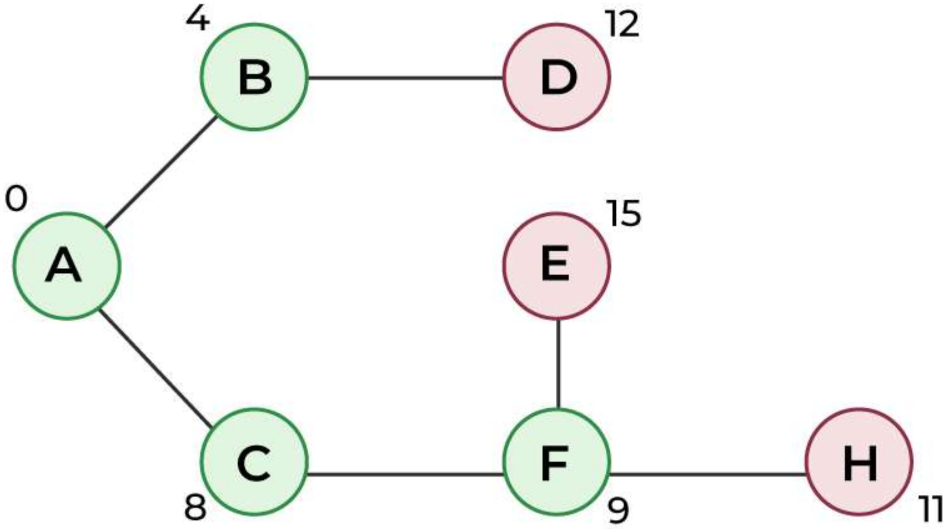
Shortest Path Calculation - Step 3

STEP 3: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 7 is picked. So sptSet now becomes {0, 1, 7}. Update the distance values of adjacent vertices of 7. The distance value of vertex 6 and 8 becomes finite (15 and 9 respectively).



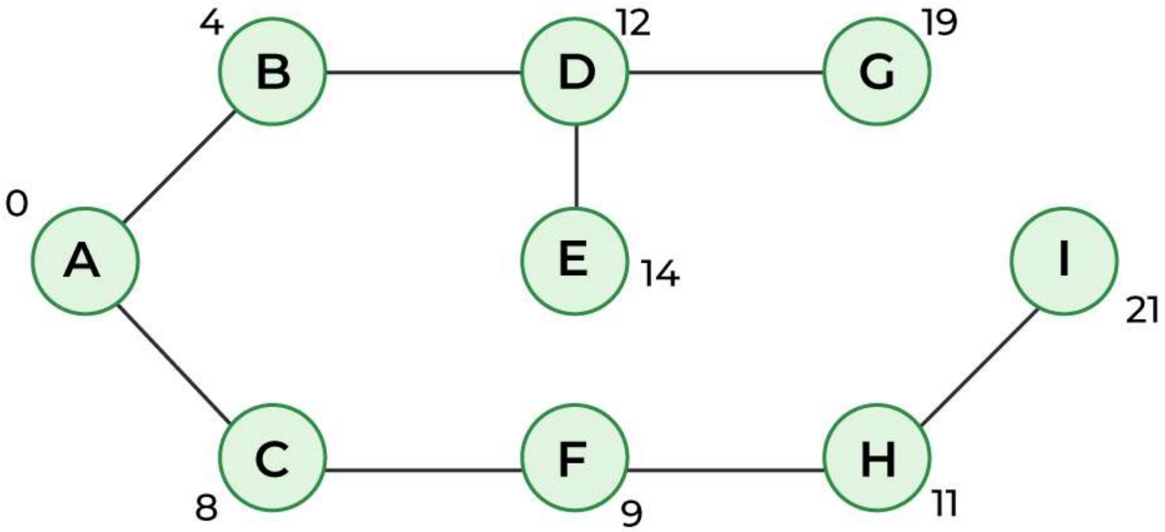
Shortest Path Calculation - Step 4

STEP 4: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 6 is picked. So sptSet now becomes {0, 1, 7, 6}. Update the distance values of adjacent vertices of 6. The distance value of vertex 5 and 8 are updated.



Shortest Path Calculation - Step 5

We repeat the above steps until sptSet includes all vertices of the given graph. Finally, we get the following Shortest Path Tree (SPT).



Shortest Path Calculation - Step 6

Characteristics of Link State Protocol

- It requires a large amount of memory.
- Shortest path computations require many CPU circles.
- If a network uses little bandwidth; it quickly reacts to topology changes
- All items in the database must be sent to neighbors to form link-state packets.
- All neighbors must be trusted in the topology.
- Authentication mechanisms can be used to avoid undesired adjacency and problems.
- No split horizon techniques are possible in the link-state routing.
- OSPF Protocol

Protocols of Link State Routing

1. Open Shortest Path First (OSPF)
2. Intermediate System to Intermediate System (IS-IS)

Open Shortest Path First (OSPF): Open Shortest Path First (OSPF) is a unicast routing protocol developed by a working group of the Internet Engineering Task Force (IETF). It is an intradomain routing protocol. It is an open-source protocol. It is similar to Routing Information Protocol (RIP). OSPF is a classless routing protocol, which means that in its updates, it includes the subnet of each route it knows about, thus, enabling variable-length subnet masks. With variable-length subnet masks, an IP network can be broken into many subnets of various sizes. This provides network administrators with extra network configuration flexibility. These updates are multicasts at specific addresses (224.0.0.5 and 224.0.0.6). OSPF is implemented as a program in the network layer using the services provided by the Internet Protocol. IP datagram that carries the messages from OSPF sets the value of the protocol field to 89. OSPF is based on the SPF algorithm, which sometimes is referred to as the Dijkstra algorithm.

Intermediate System to Intermediate System (IS-IS): Intermediate System to Intermediate System is a standardized link-state protocol that was developed as the definitive routing protocol for the OSI Model. IS-IS uses System ID to identify a router on the network. IS-IS doesn't require IP connectivity between the routers as updates are sent via CLNS instead of IP.

For more about OSPF and IS-IS, you can refer to Difference between OSPF and IS-IS.

Comment More info Advertise with us

Next Article

Distance Vector Routing (DVR) Protocol

Similar Reads

1. What is Floating Static Route ?
2. Optimized Link State Routing Protocol
3. TCL script to simulate link state routing in ns2
4. Difference between Distance vector routing and Link State routing
5. What is IP Routing?
6. Routing Tables in Computer Network
7. Securing Routing Protocols
8. Types of Routing
9. How to Add a Static Route to Windows Routing Table?

Wifi Protected Access (WPA)

Last Updated : 28 Jun, 2024

The two security protocols and security certification programs are **Wi-Fi Protected Access (WPA)** and **Wi-Fi Protected Access II (WPA2)**. These are developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these protocols because of the serious weaknesses the researchers found in the previous system, **Wired Equivalent Privacy (WEP)**. In this article, we will learn about the wep, wpa, versions of wpa, working with wpa, and how to identify the security type.

What is WEP?

Wired Equivalent Privacy (WEP) is an early security protocol for wireless networks. Introduced in 1997, WEP was designed to provide a level of security comparable to wired networks by encrypting data sent over Wi-Fi. It uses a static key to encrypt data, which is shared between devices and the wireless router. However, WEP has significant weaknesses, such as vulnerabilities to various hacking methods, making it easy for attackers to break the encryption and access the network. Because of these issues, WEP has been largely replaced by more secure protocols like WPA and WPA2.

What is Wifi Protected Access (WPA)?

WPA also referred to as the draft IEEE 802.11i standard became available in 2003. The Wi-Fi Alliance made it an intermediate measure in anticipation of the availability of the more secure and complex WPA2, which became available in 2004 and is a common short for the full IEEE 802.11i standard. In 2003, WPA also known as the TKIP standard became accessible. It was meant to be a stopgap measure by the Wi-Fi Alliance before the more complicated and secure WPA2 became available in 2004. WPA2 is a common acronym for the entire IEEE 802.11i (or IEEE 802.11i-2004) standard.

In January 2018, with several security improvements over WPA2 Wi-Fi Alliance announced the release of *WPA3*.

Versions of WPA

There are some different versions of WPA which include WPA, WPA2, and WPA3. Different versions have different features, Below mentioned are versions of WiFi Protected Access:

1. WPA

The WPA is an intermediate measure to take the place of WEP. WPA could be implemented through firmware upgrades on wireless network interface cards that were designed for WEP in 1999. However, since more changes were required in the wireless access points (APs) than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.

The WPA protocol implements almost all of the IEEE 802.11i standard. WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices which once entered can never be changed. TKIP employs a per-packet key, which means that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromise WEP.

WPA includes a Message Integrity Check, which is designed to prevent an attacker from altering or resending data packets. This replaced the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's had a main flaw in that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well-tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called TKIP to verify the integrity of the packets. TKIP is much stronger than a CRC, but the algorithm used in WPA2 is stronger. Researchers discovered a flaw in WPA similar to older weaknesses in WEP and the limitations of the message integrity code hash function, named Michael, that is used to retrieve the keystream from short packets to use for re-injection and spoofing.

2. WPA2

WPA2 replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implemented the mandatory elements of IEEE 802.11i. Particularly, it included mandatory support for CCMP(Counter Mode CBC-MAC Protocol), an AES(Advanced Encryption Standard) based encryption mode. Certification began in September 2004. WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark from March 13, 2006.

What are the New Features Does the WPA2 Protocol Offer?

WPA was replaced in 2004 with WPA2. WPA2 employs the Block Chaining Message Authentication Code Protocol (CCMP), a Counter Mode Cypher. The Advanced Encryption Standard (AES) algorithm, which verifies the authenticity and integrity of messages, forms the foundation of the CCMP protocol. Compared to the original Temporal Key Integrity Protocol (TKIP) used by WPA, CCMP is more robust and dependable.

However, WPA2 still has security flaws. The risk of unwanted access to the company wireless network is the main one among those weaknesses. This occurs when an attack vector on specific Wi-Fi Protected Setup (WPS) access points is compromised. To deter such threats, it is advised that WPS be turned off for every WPA2 attack vector access point. Threat actors can use downgrade attacks to target more vulnerabilities in WPA2.

3. WPA3

In 2018, Wi-Fi Protected Access 3, or WPA3, replaced WPA2. The most recent and improved version of WPA is WPA3. In 2018, the Wi-Fi Alliance started certifying goods that had been WPA3-approved. Not all devices immediately incorporate WPA3 capability. Users must either purchase brand-new routers that support WPA3 or have the equipment upgraded by the manufacturer in order to use WPA3-approved devices, such as wireless routers.

What are the New Features Does the WPA3 Protocol Offer?

In 2018, Wi-Fi Protected Access 3, or WPA3, replaced WPA2. WPA3 is the most recent version of the WPA protocol. In 2018, the Wi-Fi Alliance started to certify products that met WPA3 standards. Not every device has WPA3 support added to it automatically. If users want to use wireless routers or other WPA3-approved devices, they have two options: either purchase new routers that enable WPA3 or have the manufacturer update the device. A comparable 192-bit cryptographic strength (in WPA3-EAP enterprise mode), 384-bit Hashed Message Authentication Mode (HMAC), 256-bit Broadcast/Multicast Integrity Protocol (BIP-GMAC-256), 256-bit Galois/Counter Mode Protocol encryption (GCMP-256), SAE exchange, and WiFi Device Provisioning Protocol (DPP).

Working with WPA

When establishing a network for others to connect to and when connecting to a wireless network, you'll see options for employing WPA. Although it was intended to enable pre-WPA devices like those that use WEP, some only function with WPA after a firmware update. Some things are just not compatible.

Despite the protocol being more secure than WEP, attacks can still be made against WPA pre-shared keys. Your best line of defence is a passphrase that can withstand brute-force attacks.

Security Issues with WPA

- Key shared ahead of time If users rely on a weak password or passphrase, WPA and WPA2 are still susceptible to password cracking attempts.
- Insufficient upfront secrecy
- Due to the lack of forward secrecy offered by WPA and WPA2, an adversary may be able to passively and covertly gather all packets encrypted with that PSK transmitted in the past and even in the future once they ascertain the pre-shared key.
- Tactics known as denial of service, in which an attacker overloads the network with messages, impairing the availability of network resources
- Eavesdropping is the practice of unauthorised third parties intercepting data being transferred across secure networks. Spoofing and session hijacking are methods by which an attacker obtains access to network resources and data by impersonating a legitimate user.

How to Identify Your Wi-Fi Security Type?

To identify your Wi-Fi security type, follow these steps:

1. On Windows:

- Click the Wi-Fi icon in the taskbar and select your network.
- Right-click on your Wi-Fi network and select **Properties**.
- Look for the **Security type** under the "Network security settings" section.

2. On macOS:

- Click the Wi-Fi icon in the menu bar and select **Open Network Preferences**.
- Click **Advanced**, then select your network.
- Look for the **Security** field in the details.

3. On Mobile Devices:

- **iOS**: Open **Settings** > **Wi-Fi** > Tap on your network (i) > Check the **Security** field.

- **Android**: Open **Settings** > **Wi-Fi** > Tap on your network > Check the **Security** field.

4. Router Settings:

- Log in to your router's admin page (typically by entering the router's IP address in your browser).
- Navigate to the **Wireless** or **Security** settings section.
- Check the **Security Mode** or **Encryption** settings to see your Wi-Fi security type.
- Common security types include WPA2, WPA3, WEP, and WPA

Difference Between WEP and WPA

A security standard for computers with wireless internet connections is called **Wi-Fi Protected Access (WPA)**. The Wi-Fi Alliance developed it to improve upon the original Wi-Fi security standard, **Wired Equivalent Privacy (WEP)**, in terms of data encryption and user authentication.

Features	WEP	WPA
Encryption	Relies on RC4 encryption set of rules.	Supports TKIP and AES encryption algorithms for more potent protection.
Vulnerabilities	Vulnerable to numerous attacks, including brute-pressure attacks, packet sniffing, and key restoration assaults.	Addresses among the vulnerabilities found in WEP, presenting stronger safety towards attacks.

Features	WEP	WPA
Key Management	Uses static encryption keys which can be manually configured and infrequently changed.	Supports dynamic key exchange protocols, such as WPA-Personal (the use of Pre-Shared Key) or WPA-Enterprise (using IEEE 802.1X authentication), for advanced key management and protection.
Compatibility	Widely supported by older Wi-Fi devices, however compatibility can be reducing as it's far considered outdated.	Compatible with most present day Wi-Fi devices, although older devices won't aid newer encryption protocols like AES.
Security Protocol	Uses WEP encryption protocol.	Uses more potent encryption protocols inclusive of TKIP (Temporal Key Integrity Protocol) and later AES (Advanced Encryption Standard).

For more, you can refer to Difference Between WEP and WPA.

Conclusion

Wi-Fi Protected Access (WPA) improved the security of wireless networks by fixing the weaknesses in older methods like WEP. It introduced better encryption and key management. While WPA2 and WPA3 are now more commonly used because they are even more secure, WPA was an important step in making Wi-Fi safer. Knowing about WPA helps us understand why it’s important to use up-to-date security for protecting Wi-Fi connections.

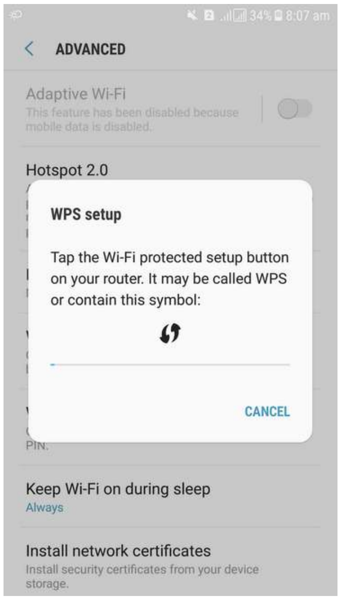
Wifi Protected Setup (WPS)

Last Updated : 08 Feb, 2024

The **Wifi protected setup (WPS)** is a wireless network security standard that tries to make connections between a router and wireless devices in a faster and easier way. WPS works only for wireless networks that use a password that is protected with the **Wifi Protected Access Personal (WPA)** or **Wifi Protected Access2 (WPA2)** Personal security protocols. WPS does not work on wireless networks that use the disfavoured Wired

An optional certification program based on a technology called Wi-Fi Protected SetupTM makes it easier to set up security-enabled Wi-Fi® networks in homes and small offices. Wi-Fi Protected Setup allows network configuration and security activation using well-known procedures (such as pressing a button or entering a PIN) that are accessible to most users.

In a standard setup, you can't connect a wireless device to a wireless network until you know the network name **(also named Service Set Identifier(SSID))** and its password (also called WPA-PSK key). If you want to connect a device, like your smartphone or a laptop, to your wireless network then on your device, you must first pick the network that you want to connect to and then enter its security password.



This feature has been disabled because mobile data is disabled.

WPS setup

Tap the Wi-Fi protected setup button on your router. It may be called WPS or contain this symbol:

Install security certificates from your device storage.

WPS

What can WPS do?

WPS can sometimes simplify the connection process. Here's how **WPS connections** can be performed:

- First, click the WPS button on your router to turn on the discovery of new devices. Then select the network you want to connect to on your device. The device is automatically connected to the wireless network without entering the network password.

- Devices like wireless printers or range extenders have their own WPS button that can be used for making quick connections. These devices can be connected to a wireless network by pressing the WPS button on the router and then on those devices. There is no need to input any data during this process. WPS automatically sends the network password, and these devices remember it for future use. The devices will be able to connect to the same network in the future without using the WPS button again.

- A third method involves the use of an eight-digit PIN. All routers with WPS enabled to have a PIN code that is generated automatically and cannot be configured by the users. This PIN can be found on the WPS configuration page on your router. Some devices are without a WPS button but with WPS support they ask for that PIN. If the pin is entered, they authenticate themselves and connect to the wireless network.

- The last method also involves using an eight-digit PIN. Some devices without a WPS button but with WPS support generate a client PIN. This PIN can be entered in your router's wireless configuration panels, and then the router will use it to add that device to the network.

The first two methods are fast but the last two methods do not provide any benefits regarding the time it takes to connect devices to your wireless network. The *eight-digit PIN* needs to be typed and typing the wireless network password is just slow. The fourth method of connecting to a wireless network is even slower because the router's wireless configuration section needs to be accessed and the PIN is to be typed provided by the client device.

WPS Operation Method

- **Push Button**: WPS capability requires the pressing of buttons located on the rear of the router and client devices. Some routers and devices have virtualized features that require activation through software on the individual devices. The device connects automatically without a password once the buttons are enabled.
- **PIN:** The access point or client device must be entered with the PIN found on the sticker that is adhered to the access point. Certain routers provide an instant PIN as soon as the device is connected, which can be used to enter the network. Devices that do not support WPS but do support the protocol use the immediate PIN feature.
- **Network Feild Communication:** To allow Near Field Communication (NFC) between a client device and an access point, the client device must be brought very close to the access point. The gadget is linked to the network and authenticated using a near field communicator. Support is offered on an optional basis. This is an out-of-band technique where the channel transfers data directly without utilising WPS.

- **USB:** Data is sent between the new device that has to be connected and the access point using a USB flash drive. Although this mode is deprecated, optional support is still offered.

Advantages of WPS

- WPS configures the network name (SSID) and WPA security key automatically for the access point having WPS enabled on the network.
- SSID security key or passphrase need not be known when connecting WPS-enabled devices.
- WPS keys are randomly generated so no one can guess or figure out your security key or passphrase.
- Long sequences of hexadecimal codes or passphrases need not be entered.
- Extensible Authentication Protocol (EAP) is used to securely exchange information and network credentials over the air, which is one of the authentication protocols used in WPA2.
- The less predictable and randomly generated key reduces the possibility of a network breach.
- removes the requirement to input a complex passphrase in hexadecimal.
- Sensitive data can be transmitted securely with WPS thanks to the introduction of Extensible Authentication Protocol (EAP) in WPA2 encryption.

Disadvantages of WPS

- Network mode where wireless devices are communicated directly to each other without an access point is not supported by WPS.
- The WPS cannot be used if WiFi devices on the network are WPS certified or WPS-compatible.
- It is very difficult to add a non-WPS client device to the network as long sequences of hexadecimal characters are generated by the WPS technology.

- The increased security offered by WPS is not available to devices that are not certified for WPS.
- The user will need to manually enter the lengthy hexadecimal passphrase on non-WPS devices.
- "Ad Hoc" connections, which let devices talk to each other directly, are not supported by WPS. Every connection needs to travel via the AP.
- WPS is still a relatively new technology, so not all devices support it.

Comment More info Advertise with us

Next Article

Wifi Protected Setup (WPS)

Similar Reads

1. Wifi Protected Access (WPA)
2. Wireless Security | Set 1
3. Wireless Security | Part 2
4. How to Set up a Secure Network?
5. Cisco Wireless Architecture and AP Modes
6. Wireless Pentest Basic
7. Wireless Communication | Set 3
8. Wireless Communication | Set 2
9. RADIUS Protocol
10. Modes of Wireless Connectivity

Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Difference Between LiFi and WiFi

Last Updated : 08 Feb, 2024

Wi-Fi(wireless fidelity) and **Li-Fi(light fidelity)** are two different technologies that are used *to send and receive data wirelessly*. In the case of Wi-Fi, we use Routers and Radio Frequency (RF) waves to transmit data, whereas in Li-Fi we use LED bulbs and Light signals to transmit and receive data.

What is WiFi?

Wireless fidelity, or wifi, is a wireless networking technique. It connects to networks and offers wireless internet using the IEEE 802.11 standard. Since cable requires installation and deployment on every computer to give an Internet connection, WiFi is more widely used because it offers a wireless connection.

Without the need for wires or cables, it functions similarly to a local area network. Wi-Fi is available on many modern computing products, including digital cameras, smart TVs, laptops, and cell phones.

Advantages of WiFi

- **Enhanced effectiveness:** Faster information transfer occurs between partners and customers as well as within firms when data connections are improved. While on a sales call, salespeople can, for instance, remotely verify prices and stock levels.
- **Savings on costs:** Installing wireless networks can be less expensive and easier, particularly in buildings that are listed or in situations where the landlord won't let wires be installed.
- **Fresh possibilities:** Using wireless networking might enable you to provide new goods or services. For instance, 'hot spot' WiFi services

have been implemented in a lot of train stations, hotels, cafes, restaurants, and airport departure lounges to enable mobile users to connect their devices to their 'home' workplaces while on the road.

- **Availability and accessibility:** You are rarely disconnected thanks to wireless technology, which enables communication while on the go and eliminates the need for additional cables or adapters to access office networks.
- **Flexibility:** While out from the office, office-based wireless workers can still be productive because they can network without occupying a separate computer. This may give rise to new working practices including working from home or having direct access to company data while at a customer's location. Find out more about workers that do remote work.

Disadvantages of WiFi

- **Security:** It is especially important to secure your wireless systems since unauthorised people are more likely to assault wireless transmissions.
- **Installation issues:** If there are additional sources of electromagnetic (radio) interference or if other people in the same building utilise wireless equipment, you can experience interference. In severe circumstances, this can result in a total loss of wireless connectivity or inadequate communication.
- **Reportage:** It might be challenging to provide reliable coverage in some buildings, which can result in "black spots" where the signal is unavailable. For instance, it could be challenging for you to hear the radio frequencies utilised in buildings constructed with steel reinforcing components.
- **Transfer rates:** Compared to 'wired' networks, wireless transmission can be less effective and slower.

What is LiFi?

Lifi, which stands for Light Fidelity, transfers and receives data via light signals and LED bulbs. Light has been used as an illumination source in homes, offices, and other spaces for a number of decades. But in the modern day, LEDs are utilised for communication in addition to lighting. LEDs are now capable of serving as a wireless communication link to access the World Wide Web from a computer or smart device.

Advantages of LiFi

- **Bandwidth and Speed:** LiFi is able to provide mobile devices with several Gbps speeds. By pushing wireless technology beyond its present limits, this next generation technology will create previously unheard-of bandwidth.
- **Security of a Military Kind:** Within a physical place, light can be secured and contained. Since LiFi provides accurate localization for asset monitoring and user authentication, it allows for much more control.
- **No Congestion:** Unlike WiFi and other RF technologies, LiFi is not affected by congestion or the negative consequences of multiuser degradation.
- **Reliable:** LiFi offers improved stability that makes it possible to communicate without interference and 1000 times more data density, which significantly enhances user experience.
- **Minimal Latency:** Presently, LiFi provides three times less latency than Wi-Fi and has the potential to significantly boost automation, creativity, and applications like augmented and virtual reality.

Disadvantages of LiFi

- Only in areas with available source light may one use the internet. Furthermore, light can only travel in a straight line of sight path and cannot pass through walls. This restricts internet access wherever it is needed. Its range is also constrained.
- It cannot be used in an outdoor setting where RF signals are present. This is a result of interference from surrounding optical sources and

sunlight. Furthermore, if it is used outside, it may be intercepted by unauthorised individuals.
- Even though it is easy to install, a Lifi system needs a completely new infrastructure. This will increase the cost for businesses or individuals wishing to use LiFi Internet service.
- Lights must be kept on day and night in order to use wifi internet services, even if it uses little power.

Difference Between LiFi and WiFi

Comparison	Li-Fi	Wi-Fi
Full form	It stands for Light Fidelity.	It stands for Wireless Fidelity.
Invented/Coined	Coined by Prof. Harald Haas in 2011.	By NCR corporation in 1991.
Operation	Using LED bulbs, it uses light to communicate data.	It transmits data using radio waves using wifi router.
Technology	Present IrDA compliant devices	WLAN 802.11/b/g/n/ac/d standard compliant devices
Data Transfer Speed	About 1 Gbps	Ranges from 150Mbps to maximum of 2Gbps
Standard	IEEE 802.15.7	IEEE 802.11
Privacy	Light is blocked by the walls hence provide	Walls cannot block radio waves so we need to employ more

Comparison	Li-Fi	Wi-Fi
	more secure data transfer.	techniques to achieve secure data transfer.
Bandwidth	Availability of unlimited bandwidth.	Availability of limited bandwidth.
Frequency of operation	10,000 times the radio's frequency spectrum	2.4Ghz, 4.9Ghz and 5Ghz
Coverage Distance	About 10 meters	About 32 meters(vary based on transmit power and antenna type)
Power Consumption	Power Consumption is Low.	Power Consumption is High.
Data density	Work with the high dense environment	Work in a less dense environment due to interference-related issues.
Cost	Low	High
Bare minimum Components used	LED bulb, LED driver and photo detector	Routers, Modems and access points
Merits	• Low cost because of VLC technology used which in turn uses highly efficient LED bulbs.	• WiFi eliminated the need for direct physical connections to access local networks and the internet without

Comparison	Li-Fi	Wi-Fi
	• Faster transmission speed as light travels at fast speed. • Less interference, ability to travel across salt water, and ability to operate in dense areas. • Prevents unauthorized access because of the no penetration feature of visible light from the opaque walls.	requiring direct physical connections to servers. Users are granted access from anywhere within range because WiFi connections are wireless. • Easy to implement as you need to contact only an Internet Service Provider (ISP) to provide an internet connection and a WiFi Router to give an access point.
Demerits	• The infrastructure required to implement LiFi technology on a large enough scale is still essentially nonexistent because it is still an emerging concept. • To enable network access, the light source must always be on. • It becomes extremely vulnerable to outside interference	• WiFi networks are notoriously insecure. Its lack of security is primarily due to its large signal range. • More interference, inability to travel over salt water, and preference for less populated areas. • Signals are highly unreliable. This is because of the fact that radio frequencies are still susceptible to numerous external

Comparison	Li-Fi	Wi-Fi
	because it uses light to communicate data. - Users are made stationary when using LiFi devices because of the short signal range emitted by light bulbs.	interferences. Due to this much range of connection issues, including weak signals, poor reception, and even connection loss can occur.
Applications	Used in airlines, undersea exploration etc.	Used for internet browsing with the help of Wifi hotspot.
Broadcast	Li-Fi uses visible light with special chips and sensors to broadcast its signal	WIFI uses radio waves to broadcast its signal.

Comment More info Advertise with us

Next Article

Difference Between LiFi and WiFi

Similar Reads

1. Difference between WiFi and MiFi
2. Difference between WiFi and GiFi
3. Difference between WiFi and WiMax
4. Difference Between WLAN and Wi-Fi
5. Difference between Wifi and Internet
6. Difference between WiFi and HotSpot
7. Difference between WiMax and LTE
8. Difference between LAN and WAN

Difference Between IPv4 and IPv6

Last Updated : 27 Dec, 2024

In the digital world, where billions of devices connect and communicate, **Internet Protocol (IP) Addresses** play a crucial role. These addresses are what allow devices to identify and locate each other on a network.

To know all about IP Addresses - refer to **What is an IP Address?**

Currently, there are **two primary versions of Internet Protocol in use: IPv4 and IPv6**. Each version has distinct characteristics, capabilities, and was developed to meet the specific needs of the internet's growth. IPv4 was the first to be widely implemented, laying the groundwork for early network communications.

However, as the internet grew and more devices started connecting online, the limitations of IPv4 became clear, leading to the creation of IPv6. This newer version was designed to address the shortcomings of its predecessor and to future-proof the network against an ever-increasing demand for more addresses and improved network efficiency.

Let’s explore their differences, why both are still in use, and the advantages each offers.

Table of Content

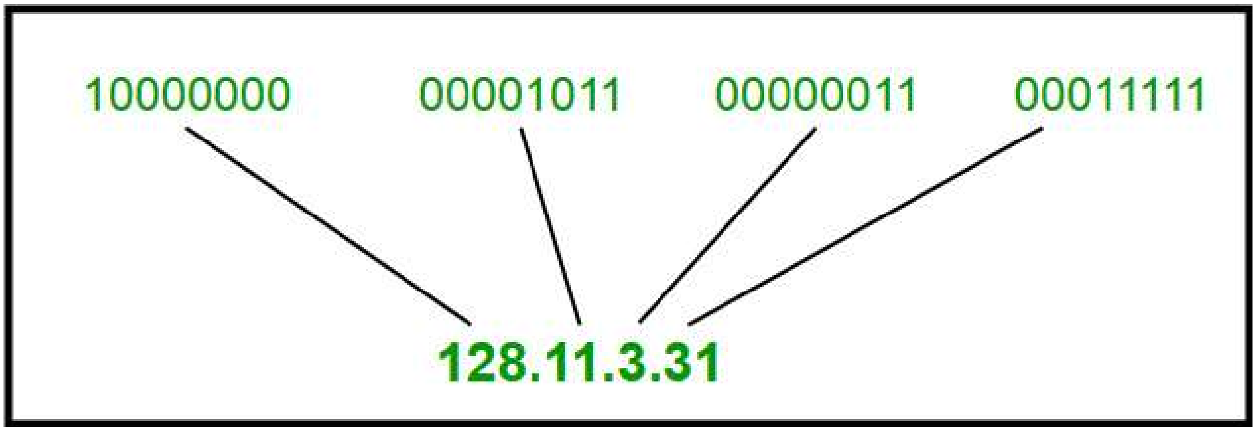
- What is IPv4?
- What is IPv6?
- Difference Between IPv4 and IPv6
- Benefits of IPv6 over IPv4
- Why IPv4 is Still in Use?

What is IPv4?

IPv4, or Internet Protocol version 4, is the original addressing system of the Internet, introduced in 1983. It uses a 32-bit address scheme, which theoretically allows for over 4 billion unique addresses (2^32). IPv4 addresses are typically displayed in decimal format, divided into four octets separated by dots. For example, 192.168.1.1 is a common IPv4 address you might find in a home network.

IPv4 Address Format

IPv4 Address Format is a 32-bit Address that comprises binary digits separated by a dot (.).



IPv4 Address Format

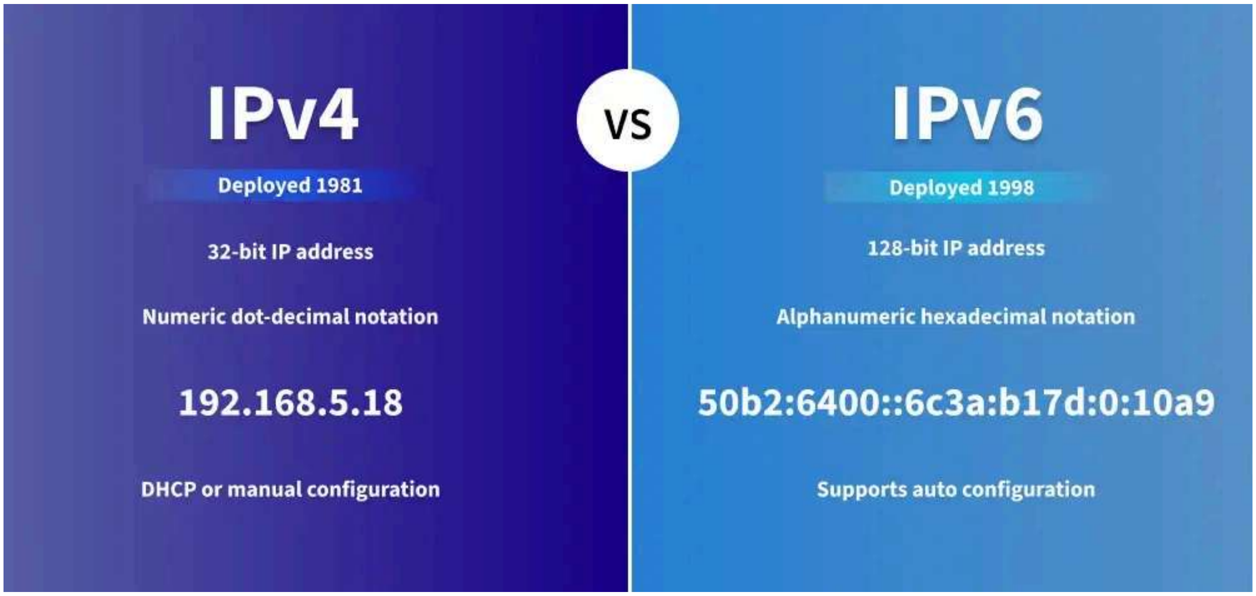
Characteristics of IPv4

- **32-bit address length**: Allows for approximately 4.3 billion unique addresses.
- **Dot-decimal notation**: IP addresses are written in a format of four decimal numbers separated by dots, such as 192.168.1.1.
- **Packet structure**: Includes a header and payload; the header contains information essential for routing and delivery.
- **Checksum fields**: Uses checksums in the header for error-checking the header integrity.
- **Fragmentation**: Allows packets to be fragmented at routers along the route if the packet size exceeds the maximum transmission unit (MTU).

- **Address Resolution Protocol (ARP)**: Used for mapping IP network addresses to the hardware addresses used by a data link protocol.
- **Manual and DHCP configuration**: Supports both manual configuration of IP addresses and dynamic configuration through DHCP (Dynamic Host Configuration Protocol).
- **Limited address space**: The main limitation which has led to the development of IPv6 to cater to more devices.
- **Network Address Translation (NAT)**: Used to allow multiple devices on a private network to share a single public IP address.
- **Security**: Lacks inherent security features, requiring additional protocols such as IPSec for secure communications.

Drawbacks of IPv4

- **Limited Address Space** : IPv4 has a limited number of addresses, which is not enough for the growing number of devices connecting to the internet.
- **Complex Configuration** : IPv4 often requires manual configuration or DHCP to assign addresses, which can be time-consuming and prone to errors.
- **Less Efficient Routing** : The IPv4 header is more complex, which can slow down data processing and routing.
- **Security Issues** : IPv4 does not have built-in security features, making it more vulnerable to attacks unless extra security measures are added.
- **Limited Support for Quality of Service (QoS)** : IPv4 has limited capabilities for prioritizing certain types of data, which can affect the performance of real-time applications like video streaming and VoIP.
- **Fragmentation** : IPv4 allows routers to fragment packets, which can lead to inefficiencies and increased chances of data being lost or corrupted.
- **Broadcasting Overhead** : IPv4 uses broadcasting to communicate with multiple devices on a network, which can create unnecessary network traffic and reduce performance.


IPv4
Deployed 1981
32-bit IP address
Numeric dot-decimal notation
192.168.5.18
DHCP or manual configuration
VS
IPv6
Deployed 1998
128-bit IP address
Alphanumeric hexadecimal notation
50b2:6400::6c3a:b17d:0:10a9
Supports auto configuration

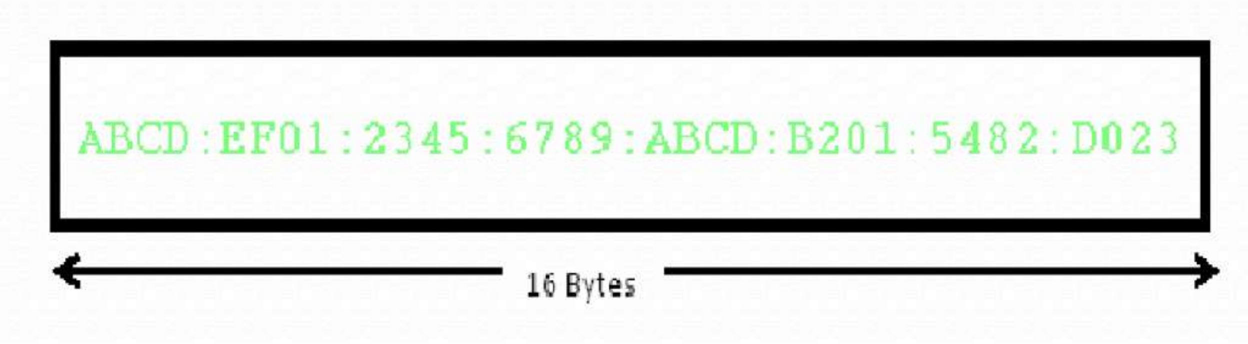
What is IPv6?

Another most common version of the Internet Protocol currently is IPv6. The well-known IPv6 protocol is being used and deployed more often, especially in mobile phone markets. IPv6 was designed by the Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding IPv4 due to the global exponentially growing internet of users.

IPv6 stands for Internet Protocol version 6. IPv6 is the new version of Internet Protocol, which is way better than IPv4 in terms of complexity and efficiency. IPv6 is written as a group of 8 hexadecimal numbers separated by colon (:). It can be written as 128 bits of 0s and 1s.

IPv6 Address Format

IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).


ABCD:EF01:2345:6789:ABCD:B201:5482:D023
16 Bytes

IPv6 Address Format

To switch from IPv4 to IPv6, there are several strategies:

- **Dual Stacking** : Devices can use both IPv4 and IPv6 at the same time. This way, they can talk to networks and devices using either version.
- **Tunneling** : This method allows IPv6 users to send data through an IPv4 network to reach other IPv6 users. Think of it as creating a "tunnel" for IPv6 traffic through the older IPv4 system.
- **Network Address Translation (NAT)** : NAT helps devices using different versions of IP addresses (IPv4 and IPv6) to communicate with each other by translating the addresses so they understand each other.

Characteristics of IPv6

- IPv6 uses 128-bit addresses, offering a much larger address space than IPv4's 32-bit system.
- IPv6 addresses use a combination of numbers and letters separated by colons, allowing for more unique addresses.
- The IPv6 header has fewer fields, making it more efficient for routers to process.
- IPv6 supports Unicast, Multicast, and Anycast, but no Broadcast, reducing network traffic.
- IPv6 allows flexible subnetting (VLSM) to divide networks based on specific needs.
- IPv6 uses Neighbor Discovery for MAC address resolution instead of ARP.
- IPv6 uses advanced routing protocols like OSPFv3 and RIPng for better address handling.
- IPv6 devices can self-assign IP addresses using SLAAC, or use DHCPv6 for more control.
- IPv6 handles fragmentation at the sender side, not by routers, improving speed.

Difference Between IPv4 and IPv6

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
It can generate 4.29x10 ^{9} address space	The address space of IPv6 is quite large it can produce 3.4x10 ^{38} address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available

IPv4	IPv6
It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.
IPv4 supports VLSM(Variable Length subnet mask).	IPv6 does not support VLSM.
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

Benefits of IPv6 over IPv4

The recent Version of IP IPv6 has a greater advantage over IPv4. Here are some of the mentioned benefits:

- **Larger Address Space:** IPv6 has a greater address space than IPv4, which is required for expanding the IP Connected Devices. IPv6 has 128 bit IP Address rather and IPv4 has a 32-bit Address.
- **Improved Security:** IPv6 has some improved security which is built in with it. IPv6 offers security like Data Authentication, Data Encryption, etc. Here, an Internet Connection is more Secure.
- **Simplified Header Format:** As compared to IPv4, IPv6 has a simpler and more effective header Structure, which is more cost-effective and also increases the speed of Internet Connection.
- **Prioritize:** IPv6 contains stronger and more reliable support for QoS features, which helps in increasing traffic over websites and increases audio and video quality on pages.
- **Improved Support for Mobile Devices:** IPv6 has increased and better support for Mobile Devices. It helps in making quick connections over other Mobile Devices and in a safer way than IPv4.

Why IPv4 is Still in Use?

1. **Infrastructure Compatibility** Many systems and devices are built for IPv4 and require significant updates to support IPv6, including routers, switches, and computers.
2. **Cost of Transition** - Switching to IPv6 can be expensive and complex, involving hardware updates, software upgrades, and training for personnel.
3. **Lack of Immediate Need** - Techniques like NAT (Network Address Translation) help extend the life of IPv4 by allowing multiple devices to share a single public IP address, reducing the urgency to switch to IPv6.
4. **Coexistence Strategies** - Technologies that allow IPv4 and IPv6 to run simultaneously make it easier for organizations to adopt IPv6 gradually while maintaining their existing IPv4 systems.
5. **Slow Global Adoption** - The adoption of IPv6 varies significantly around the world, which necessitates the continued support of IPv4 for

global connectivity.

6. **Lack of Visible Benefits** - Many users and organizations don't see immediate improvements with IPv6 if they don't face an IP address shortage, reducing the incentive to upgrade.

Conclusion

The shift from IPv4 to IPv6 is more than just an expansion of address space; it represents a necessary evolution in internet architecture to accommodate future growth and innovation. Understanding these differences helps not only in appreciating how the internet works but also in foreseeing how technology will continue to evolve to meet the needs of an increasingly connected world.

Comment More info Advertise with us

Next Article

Global Unicast Address in CCNA

GeeksforGeeks
SanchhayaEducation Private Limited

Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Registered Address:
K 061, Tower K, Gulshan Vivante
Apartment, Sector 137, Noida, Gautam
Buddh Nagar, Uttar Pradesh, 201305

GET IT ON Google Play Download on the App Store

Advertise with us

TCP Connection Establishment

Last Updated : 21 May, 2025

TCP (Transmission Control Protocol) is a core internet protocol that ensures reliable, ordered, and error-checked delivery of data between computers. It establishes a connection using a three-way handshake before data transfer begins, allowing both devices to synchronize and agree on communication parameters. TCP breaks data into packets, manages their delivery by resending lost packets, and reassembles them in the correct order. This makes TCP ideal for applications like web browsing, email, and file transfers where accuracy and reliability are important.

TCP Connection Establishment

1. Sender starts the process with the following:

- **Sequence number (Seq=521):** contains the random initial sequence number generated at the sender side.
- **Syn flag (Syn=1):** request the receiver to synchronize its sequence number with the above-provided sequence number.
- **Maximum segment size (MSS=1460 B):** sender tells its maximum segment size, so that receiver sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.
- **Window size (window=14600 B):** sender tells about his buffer capacity in which he has to store messages from the receiver.

2. TCP is a full-duplex protocol so both sender and receiver require a window for receiving messages from one another.

- **Sequence number (Seq=2000):** contains the random initial sequence number generated at the receiver side.

- **Syn flag (Syn=1):** request the sender to synchronize its sequence number with the above-provided sequence number.
- **Maximum segment size (MSS=500 B):** receiver tells its maximum segment size, so that sender sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header. Since MSS $_{receiver}$ < MSS $_{sender}$, both parties agree for minimum MSS i.e., 500 B to avoid fragmentation of packets at both ends.

  Therefore, receiver can send maximum of 14600/500 = 29 packets. This is the receiver's sending window size.

- **Window size (window=10000 B):** receiver tells about his buffer capacity in which he has to store messages from the sender.

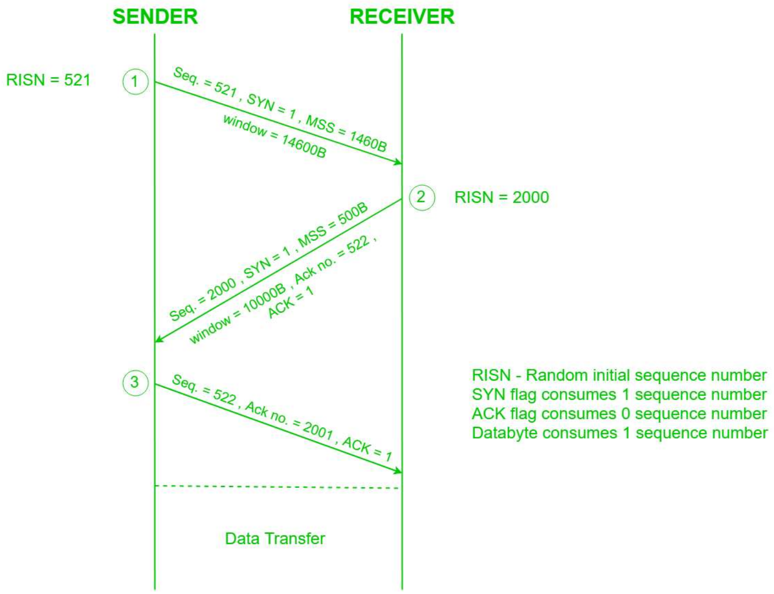
  Therefore, sender can send a maximum of 10000/500 = 20 packets. This is the sender's sending window size.

- **Acknowledgement Number (Ack no.=522):** Since sequence number 521 is received by the receiver so, it makes a request for the next sequence number with Ack no.=522 which is the next packet expected by the receiver since Syn flag consumes 1 sequence no.
- **ACK flag (ACk=1):** tells that the acknowledgement number field contains the next sequence expected by the receiver.

3. Sender makes the final reply for connection establishment in the following way:

- **Sequence number (Seq=522):** since sequence number = 521 in 1 st step and SYN flag consumes one sequence number hence, the next sequence number will be 522.
- **Acknowledgement Number (Ack no.=2001):** since the sender is acknowledging SYN=1 packet from the receiver with sequence number 2000 so, the next sequence number expected is 2001.

- **ACK flag (ACK=1):** tells that the acknowledgement number field contains the next sequence expected by the sender.


SENDER
RECEIVER
RISN = 521
①
Seq. = 521 , SYN = 1 , MSS = 1460B
window = 14600B
②
RISN = 2000
Seq. = 2000 , SYN = 1 , MSS = 500B
window = 10000B , Ack no. = 522 ,
ACK = 1
③
Seq. = 522 , Ack no. = 2001 , ACK = 1
RISN - Random initial sequence number
SYN flag consumes 1 sequence number
ACK flag consumes 0 sequence number
Databyte consumes 1 sequence number
Data Transfer

Since the connection establishment phase of TCP makes use of 3 packets, it is also known as 3-way Handshaking **(SYN, SYN + ACK, ACK).**

TCP Flags Used in Connection Establishment

TCP uses special flags to manage connections between devices such as:

- **SYN (Synchronize):** This flag is used to start a new connection between two devices.
- **ACK (Acknowledge):** It confirms that a message has been received successfully.
- **RST (Reset):** This flag is used to abruptly close a connection due to errors or security reasons.
- **FIN (Finish):** It signals that one device wants to close the connection properly.

Common Issues in TCP Connection Establishment

Sometimes, problems can occur while setting up a connection. Here are some common issues:

- **SYN Flood Attacks:** Hackers send many SYN requests without completing the connection, overloading the server.

- **Connection Timeout:** If a device does not respond in time, the connection attempt fails.
- **Packet Loss:** Some data packets might get lost due to network issues, causing delays or failures in connection.

How to Optimize TCP Connection Establishment?

To make TCP connections faster and more reliable, here are some useful methods:

- **Reducing Latency with TCP Fast Open:** This allows data to be sent earlier, reducing the delay when starting a connection.
- **Using Keep-Alive Mechanism:** This keeps connections open longer, avoiding the need to set up new ones repeatedly.
- **Load Balancing for Faster Handshakes:** Distributing traffic across multiple servers helps in handling many connections efficiently.

Practice GATE IT 2008 | Question 67 based on three-way handshake process.

> *Also, read about TCP Connection Termination.*

What does "established" mean in TCP?

> *"Established" in TCP means a connection is successfully set up between two devices, allowing data transfer after completing the three-way handshake.*

What is the TCP connection limit?

> *The limit depends on system resources and configurations, but most modern systems support thousands to millions of concurrent connections.*

What is the speed limit of a TCP connection?

> *TCP speed depends on factors like network bandwidth, latency, congestion, and window size, but it has no fixed limit.*

Transport Layer responsibilities

Last Updated : 30 Sep, 2024

The transport Layer is the second layer in the TCP/IP model and the fourth layer in the OSI model. It is an end-to-end layer used to deliver messages to a host. It is termed an end-to-end layer because it provides a point-to-point connection rather than hop-to-hop, between the source host and destination host to deliver the services reliably. The unit of data encapsulation in the Transport Layer is a segment.

Working of Transport Layer

The transport layer takes services from the Application layer and provides services to the Network layer.

The transport layer ensures the reliable transmission of data between systems. Understanding protocols like **TCP** and **UDP** is crucial. If you're aiming for a deeper understanding of transport layer protocols, the **GATE CS Self-Paced Course** offers comprehensive modules on networking, including detailed explanations of transport layer responsibilities and how they operate in real-world applications.

At the sender's side: The transport layer receives data (message) from the Application layer and then performs Segmentation, divides the actual message into segments, adds the source and destination's port numbers into the header of the segment, and transfers the message to the Network layer.

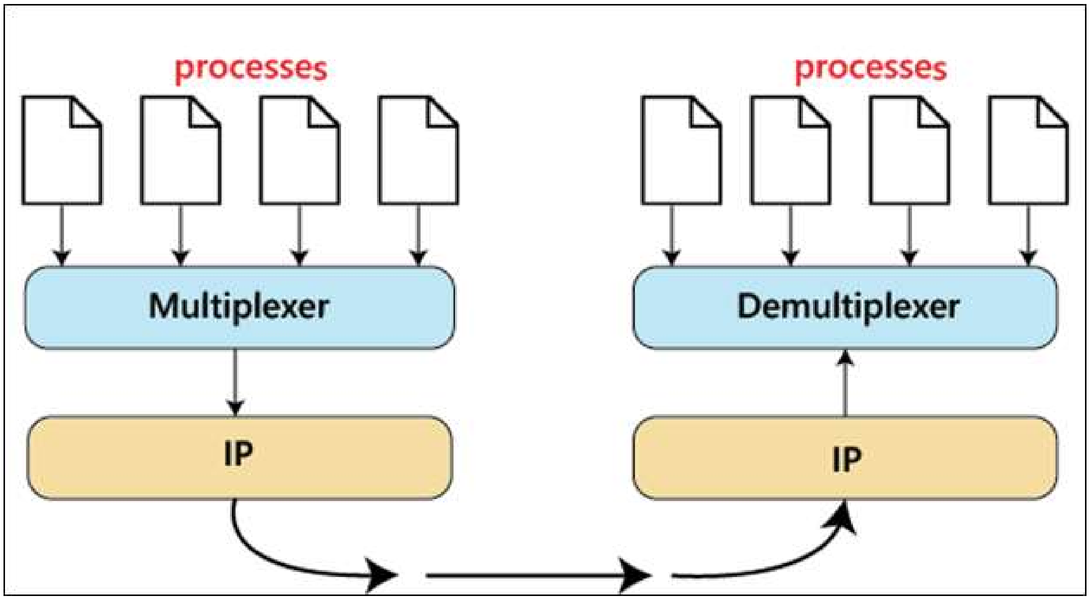
At the receiver's side: The transport layer receives data from the Network layer, reassembles the segmented data, reads its header, identifies the port number, and forwards the message to the appropriate port in the Application layer.

Responsibilities of a Transport Layer

- The Process to Process Delivery
- End-to-End Connection between Hosts
- Multiplexing and Demultiplexing
- Congestion Control
- Data integrity and Error correction
- Flow control

1. The Process to Process Delivery

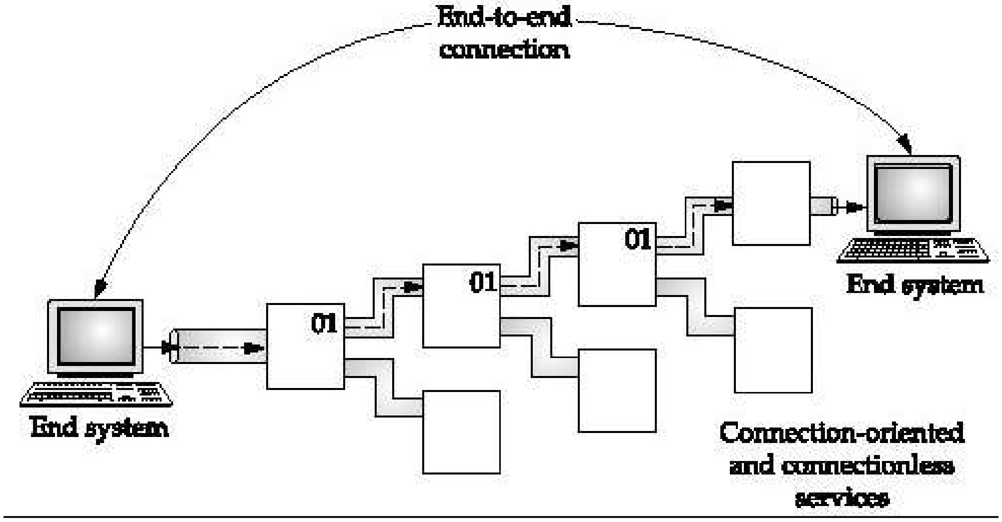
While Data Link Layer requires the MAC address (48 bits address contained inside the Network Interface Card of every host machine) of source-destination hosts to correctly deliver a frame and the Network layer requires the IP address for appropriate routing of packets, in a similar way Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A port number is a 16-bit address used to identify any client-server program uniquely.



Process to Process Delivery

2. End-to-end Connection between Hosts

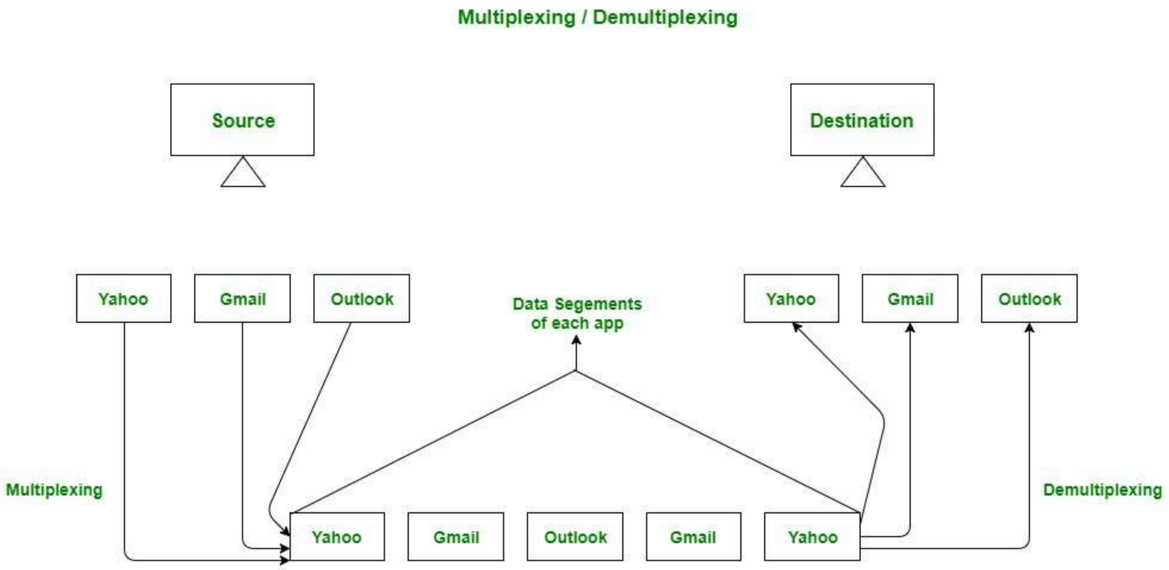
The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection-orientated protocol that uses a handshake protocol to establish a robust connection between two end hosts. TCP ensures the reliable delivery of messages and is used in various applications. UDP, on the other hand, is a stateless and unreliable protocol that ensures best-effort delivery. It is suitable for applications that have little concern with flow or error control and requires sending the bulk of data like video conferencing. It is often used in multicasting protocols.



End to End Connection.

3. Multiplexing and Demultiplexing

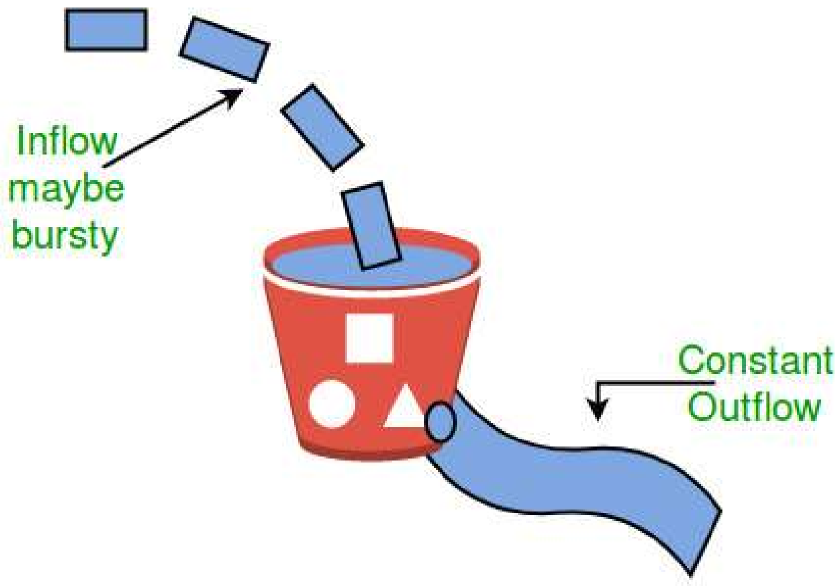
Multiplexing(many to one) is when data is acquired from several processes from the sender and merged into one packet along with headers and sent as a single packet. Multiplexing allows the simultaneous use of different processes over a network that is running on a host. The processes are differentiated by their port numbers. Similarly, Demultiplexing(one to many) is required at the receiver side when the message is distributed into different processes. Transport receives the segments of data from the network layer distributes and delivers it to the appropriate process running on the receiver's machine.


Multiplexing / Demultiplexing
Source
Destination
Yahoo
Gmail
Outlook
Data Segements of each app
Yahoo
Gmail
Outlook
Multiplexing
Demultiplexing
Yahoo
Gmail
Outlook
Gmail
Yahoo

Multiplexing and Demultiplexing

4. Congestion Control

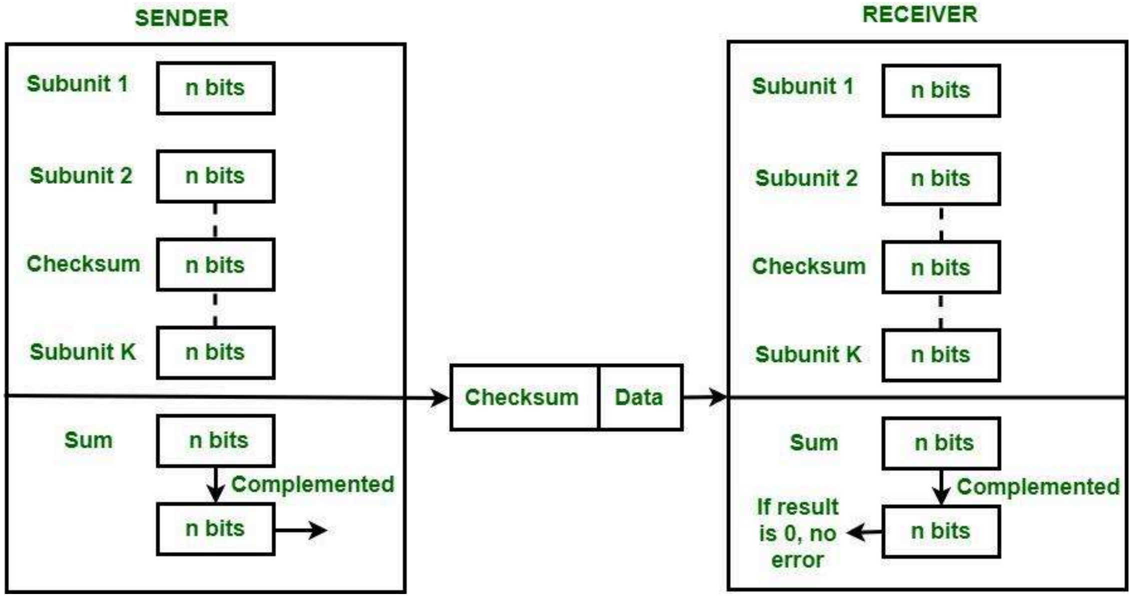
Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occurs. As a result, the retransmission of packets from the sources increases the congestion further. In this situation, the Transport layer provides Congestion Control in different ways. It uses open-loop congestion control to prevent congestion and closed-loop congestion control to remove the congestion in a network once it occurred. TCP provides AIMD - additive increases multiplicative decrease and leaky bucket technique for congestion control.


Inflow maybe bursty
Constant Outflow

Leaky Bucket Congestion Control Technique

5. Data integrity and Error Correction

The transport layer checks for errors in the messages coming from the application layer by using error detection codes, and computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.


SENDER
Subunit 1
n bits
Subunit 2
n bits
Checksum
n bits
Subunit K
n bits
Sum
n bits
Complemented
n bits
Checksum
Data
RECEIVER
Subunit 1
n bits
Subunit 2
n bits
Checksum
n bits
Subunit K
n bits
Sum
n bits
Complemented
If result is 0, no error
n bits

Error Correction using Checksum

6. Flow Control

The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

Protocols of Transport Layer

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Stream Control Transmission Protocol (SCTP)

Multiplexing and Demultiplexing in Transport Layer

Last Updated : 28 Dec, 2024

Multiplexing and Demultiplexing services are provided in almost every protocol architecture ever designed. UDP and TCP perform the demultiplexing and multiplexing jobs by including two special fields in the segment headers: the source port number field and the destination port number field.

Multiplexing -
Gathering data from multiple application processes of the sender, enveloping that data with a header, and sending them as a whole to the intended receiver is called multiplexing.

Demultiplexing -
Delivering received segments at the receiver side to the correct app layer processes is called demultiplexing.

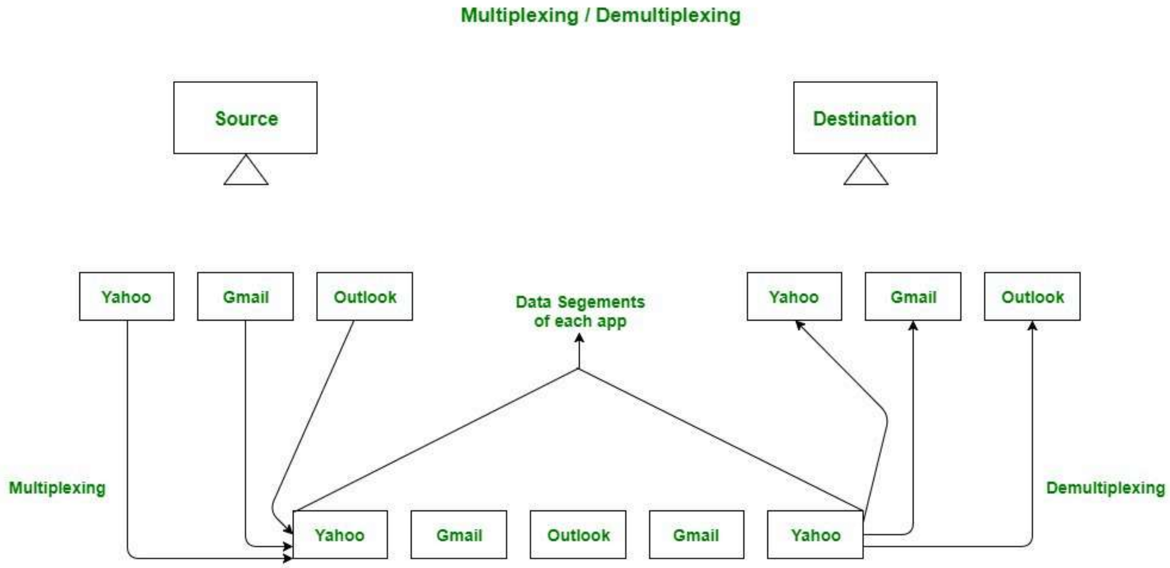

Multiplexing / Demultiplexing
Source
Destination
Yahoo
Gmail
Outlook
Data Segements of each app
Yahoo
Gmail
Outlook
Multiplexing
Demultiplexing
Yahoo
Gmail
Outlook
Gmail
Yahoo

Figure - Abstract view of multiplexing and demultiplexing

Multiplexing and demultiplexing are the services facilitated by the transport layer of the OSI model.

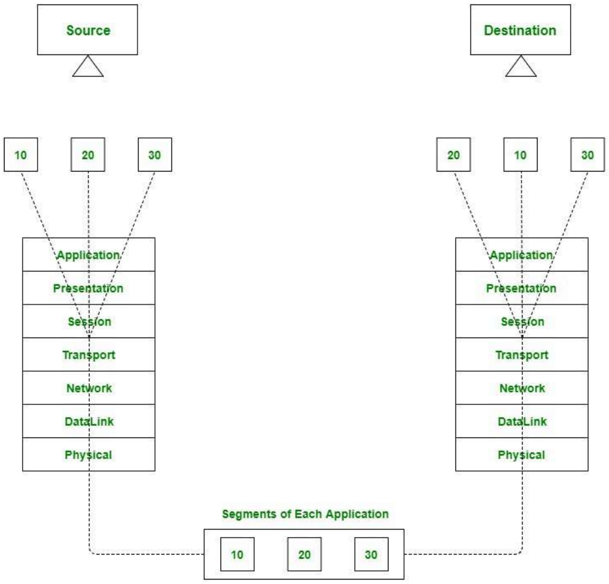
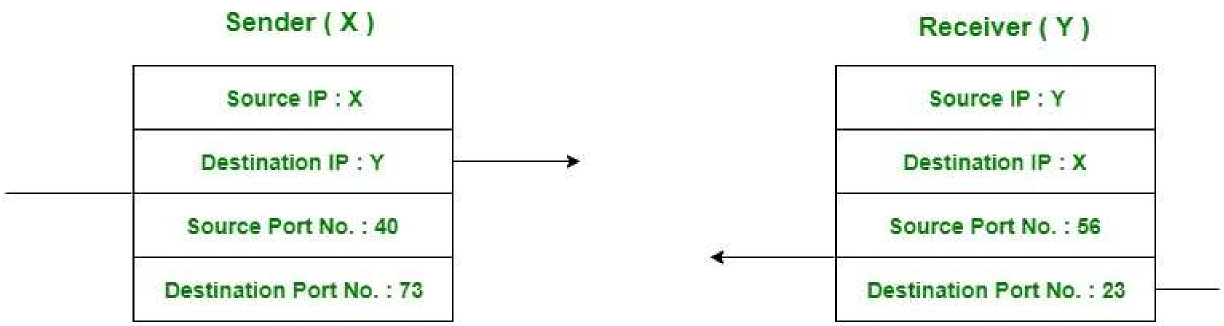

Source
Destination
10
20
30
20
10
30
Application
Presentation
Session
Transport
Network
DataLink
Physical
Application
Presentation
Session
Transport
Network
DataLink
Physical
Segments of Each Application
10
20
30

Figure - Transport layer- junction for multiplexing and demultiplexing

There are two types of multiplexing and Demultiplexing :

1. Connectionless Multiplexing and Demultiplexing
2. Connection-Oriented Multiplexing and Demultiplexing

How Multiplexing and Demultiplexing is done -
For sending data from an application on the sender side to an application at the destination side, the sender must know the IP address of the destination and port number of the application (at the destination side) to which he wants to transfer the data. Block diagram is shown below :



Sender (X)
Source IP : X
Destination IP : Y
Source Port No. : 40
Destination Port No. : 73
Receiver (Y)
Source IP : Y
Destination IP : X
Source Port No. : 56
Destination Port No. : 23

Figure - Transfer of packet between applications of sender and receiver

Let us consider two messaging apps that are widely used nowadays viz. Hike and WhatsApp. Suppose A is the sender and B is the receiver. Both sender and receiver have these applications installed in their system (say smartphone). Suppose A wants to send messages to B in WhatsApp and hike both. In order to do so, A must mention the IP address of B and destination port number of the WhatsApp while sending the message through the WhatsApp application. Similarly, for the latter case, A must mention the IP address of B and the destination port number of the hike while sending the message.

Now the messages from both the apps will be wrapped up along with appropriate headers(viz. source IP address, destination IP address, source port no, destination port number) and sent as a single message to the receiver. This process is called multiplexing. At the destination, the received message is unwrapped and constituent messages (viz messages from a hike and WhatsApp application) are sent to the appropriate application by looking to the destination the port number. This process is called demultiplexing. Similarly, B can also transfer the messages to A.

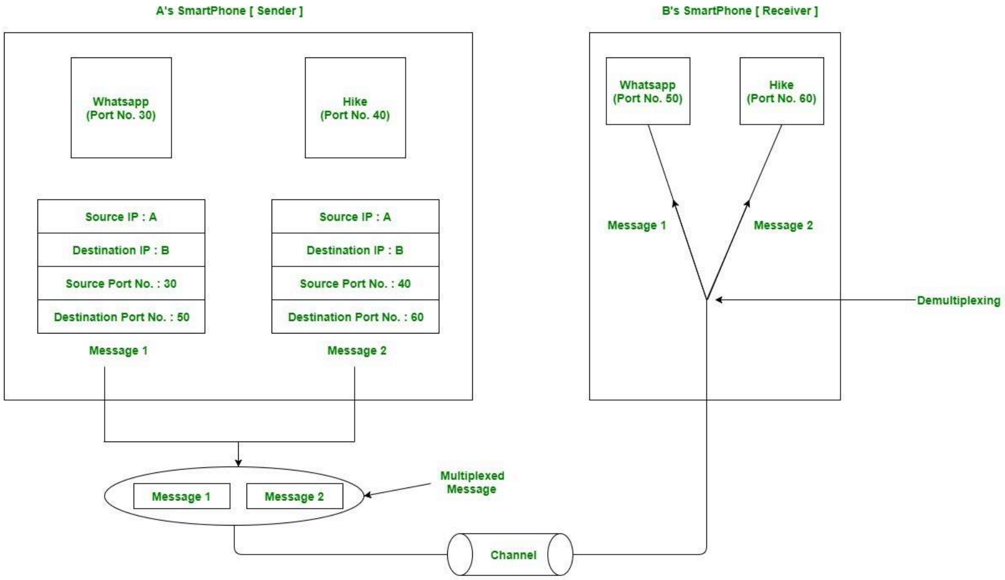

A's SmartPhone [Sender]
Whatsapp (Port No. 30)
Hike (Port No. 40)
Source IP : A
Destination IP : B
Source Port No. : 30
Destination Port No. : 50
Message 1
Source IP : A
Destination IP : B
Source Port No. : 40
Destination Port No. : 60
Message 2
Message 1
Message 2
Multiplexed Message
Channel
B's SmartPhone [Receiver]
Whatsapp (Port No. 50)
Hike (Port No. 60)
Message 1
Message 2
Demultiplexing

Figure - Message transfer using WhatsApp and hike messaging application

References -

[Multiplexing/Demultiplexing](#)
[dcs.bbk.ac.uk](#)

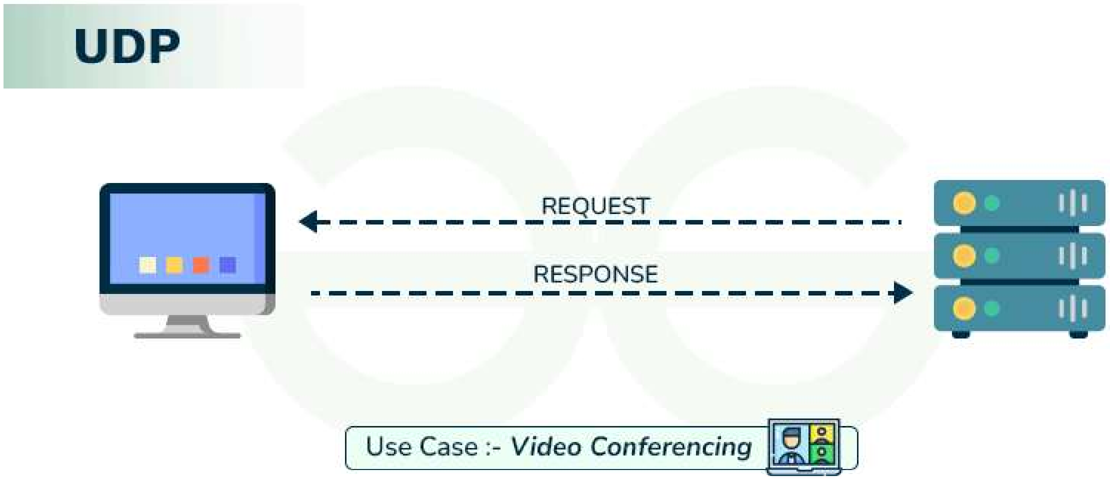
User Datagram Protocol (UDP)

Last Updated : 27 Dec, 2024

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an **unreliable and connectionless protocol.** So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections over the network. The UDP enables process-to-process communication.

What is User Datagram Protocol?

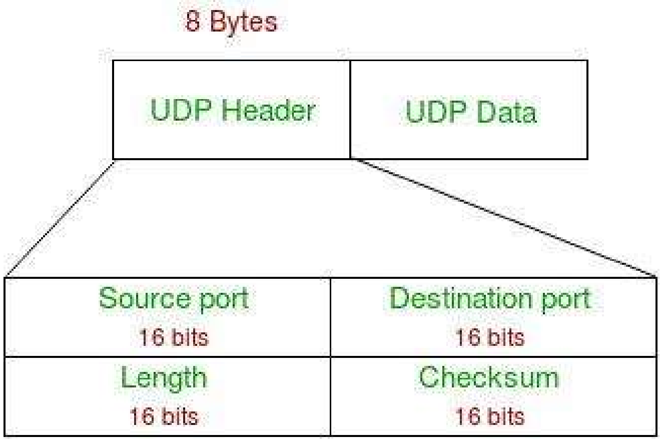
User Datagram Protocol (UDP) is one of the core protocols of the Internet Protocol (IP) suite. It is a communication protocol used across the internet for time-sensitive transmissions such as video playback or DNS lookups . Unlike Transmission Control Protocol (TCP), UDP is connectionless and does not guarantee delivery, order, or error checking, making it a lightweight and efficient option for certain types of data transmission.



Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw

UDP Header

UDP header is an **8-byte** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contain all necessary header information and the remaining part consists of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.



UDP Header

- **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
- **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
- **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
- **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Notes - Unlike TCP, the Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting. Also UDP provides port numbers so that is can differentiate between users requests.

Applications of UDP

- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.
- VoIP (Voice over Internet Protocol) services, such as Skype and WhatsApp, use UDP for real-time voice communication. The delay in voice communication can be noticeable if packets are delayed due to congestion control, so UDP is used to ensure fast and efficient data transmission.
- DNS (Domain Name System) also uses UDP for its query/response messages. DNS queries are typically small and require a quick response time, making UDP a suitable protocol for this application.
- DHCP (Dynamic Host Configuration Protocol) uses UDP to dynamically assign IP addresses to devices on a network. DHCP messages are typically small, and the delay caused by packet loss or retransmission is generally not critical for this application.
- Following implementations uses UDP as a transport layer protocol:
    - NTP (Network Time Protocol)
    - DNS (Domain Name Service)
    - BOOTP, DHCP.
    - NNP (Network News Protocol)
    - Quote of the day protocol
    - TFTP, RTSP, RIP.
- The application layer can do some of the tasks through UDP-
    - Trace Route
    - Record Route
    - Timestamp

- UDP takes a datagram from Network Layer , attaches its header, and sends it to the user. So, it works fast.

TCP vs UDP

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error-checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission	There is no sequencing of data in UDP. If the

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
	Control Protocol (TCP). this means that packets arrive in order at the receiver.	order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.
Protocols	TCP is used by HTTP, HTTPs , FTP , SMTP and Telnet .	UDP is used by DNS, DHCP, TFTP, SNMP , RIP, and VoIP.
Stream Type	The TCP connection is a byte stream.	UDP connection is a message stream.

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Overhead	Low but higher than UDP.	Very low.
Applications	This protocol is primarily utilized in situations when a safe and trustworthy communication procedure is necessary, such as in email, on the web surfing, and in military services.	This protocol is used in situations where quick communication is necessary but where dependability is not a concern, such as VoIP, game streaming, video, and music streaming, etc.

Advantages of UDP

- **Speed:** UDP is faster than TCP because it does not have the overhead of establishing a connection and ensuring reliable data delivery.
- Lower latency: Since there is no connection establishment, there is lower latency and faster response time.
- **Simplicity:** UDP has a simpler protocol design than TCP, making it easier to implement and manage.
- **Broadcast support:** UDP supports broadcasting to multiple recipients, making it useful for applications such as video streaming and online gaming.
- **Smaller packet size:** UDP uses smaller packet sizes than TCP, which can reduce network congestion and improve overall network performance.
- User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

Disadvantages of UDP

- **No reliability:** UDP does not guarantee delivery of packets or order of delivery, which can lead to missing or duplicate data.
- **No congestion control:** UDP does not have congestion control, which means that it can send packets at a rate that can cause network congestion.
- **Vulnerable to attacks:** UDP is vulnerable to denial-of-service attacks , where an attacker can flood a network with UDP packets, overwhelming the network and causing it to crash.
- **Limited use cases:** UDP is not suitable for applications that require reliable data delivery, such as email or file transfers, and is better suited for applications that can tolerate some data loss, such as video streaming or online gaming.

How is UDP used in DDoS attacks?

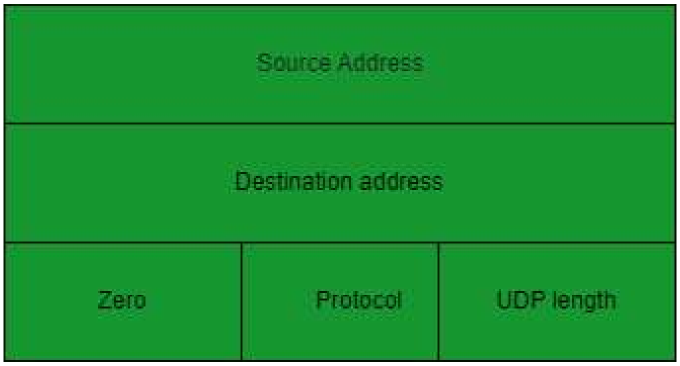
A **UDP flood attack** is a type of **Distributed Denial of Service (DDoS)** attack where an attacker sends a large number of **User Datagram Protocol (UDP)** packets to a target port.

- **UDP Protocol** : Unlike TCP, UDP is connectionless and doesn’t require a handshake before data transfer. When a UDP packet arrives at a server, it checks the specified port for listening applications. If no app is found, the server sends an ICMP **“destination unreachable”** packet to the supposed sender (usually a random bystander due to spoofed IP addresses).
- **Attack Process** :
    - The attacker sends UDP packets with spoofed IP sender addresses to random ports on the target system.
    - The server checks each incoming packet’s port for a listening application (usually not found due to random port selection).
    - The server sends ICMP “destination unreachable” packets to the spoofed sender (random bystanders).
    - The attacker floods the victim with UDP data packets, overwhelming its resources.

- **Mitigation** : To protect against UDP flood attacks, monitoring network traffic for sudden spikes and implementing security measures are crucial. Organizations often use specialized tools and services to detect and mitigate such attacks effectively.

UDP Pseudo Header

- The purpose of using a pseudo-header is to verify that the UDP packet has reached its correct destination
- The correct destination consist of a specific machine and a specific protocol port number within that machine



UDP pseudo header

UDP Pseudo Header Details

- The UDP header itself specify only protocol port number.thus , to verify the destination UDP on the sending machine computes a checksum that covers the destination IP address as well as the UDP packet.
- At the ultimate destination, UDP software verifies the checksum using the destination IP address obtained from the header of the IP packet that carried the UDP message.
- If the checksum agrees, then it must be true that the packet has reached the intended destination host as well as the correct protocol port within that host.

User Interface

A user interface should allow the creation of new receive ports, receive operations on the receive ports that returns the data octets and an indication of source port and source address, and an operation that allows a datagram to be sent, specifying the data, source and destination ports and address to be sent.

IP Interface

- The UDP module must be able to determine the source and destination internet address and the protocol field from internet header
- One possible UDP/IP interface would return the whole internet datagram including the entire internet header in response to a receive operation
- Such an interface would also allow the UDP to pass a full internet datagram complete with header to the IP to send. the IP would verify certain fields for consistency and compute the internet header checksum.
- The IP interface allows the UDP module to interact with the network layer of the protocol stack, which is responsible for routing and delivering data across the network.
- The IP interface provides a mechanism for the UDP module to communicate with other hosts on the network by providing access to the underlying IP protocol.
- The IP interface can be used by the UDP module to send and receive data packets over the network, with the help of IP routing and addressing mechanisms.

GATE Questions for Practice

- GATE CS 2013, Question 12
- GATE CS 2012, Question 65
- GATE CS 2007, Question 20
- GATE CS 2005, Question 23
- GATE IT 2008, Question 66

- GATE Mock 2015, Question 5

Conclusion

The User Datagram Protocol (UDP) is an important Transport Layer protocol in the Internet Protocol (IP) suite, identified for its speed and efficiency due to its connectionless and lightweight design. While UDP lacks TCP's stability and error-checking features, it used in applications that need low latency and real-time performance, such as streaming, online gaming, and DNS lookups. Its simplicity and support for broadcast and multicast broadcasts make it a useful tool for specialized applications, despite its vulnerability to data loss and network congestion.

Comment More info Advertise with us

Next Article

IPv4 Datagram Header

Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Registered Address:
K 061, Tower K, Gulshan Vivante
Apartment, Sector 137, Noida, Gautam
Buddh Nagar, Uttar Pradesh, 201305

GET IT ON Google Play Download on the App Store

Advertise with us

Search...

53

P2P (Peer To Peer) File Sharing

Last Updated : 23 Jul, 2023

In Computer Networking, P2P (Peer-to-Peer) is a file-sharing technology, that allows users to access mainly the multimedia files like videos, music, e-books, games, etc. The individual users in this network are referred to as

Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw

UDP connections.

How Does P2P (Peer-to-Peer) Work?

A peer-to-peer network allows computer hardware and software to communicate without the need for a server. Unlike client-server architecture, there is no central server for processing requests in a P2P architecture. The peers directly interact with one another without the requirement of a central server.

Now, when one peer makes a request, multiple peers may have a copy of that requested object. Now the problem is how to get the IP addresses of all those peers. This is decided by the underlying architecture supported by the P2P systems. Using one of these methods, the client peer can get to know all the peers which have the requested object/file and the file transfer takes place directly between these two peers.

P2P Architecture

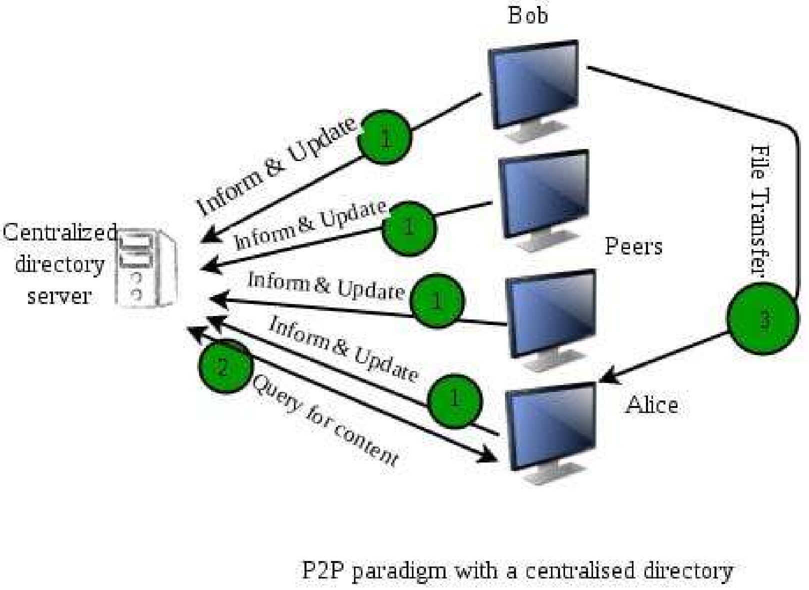
1. Centralized Directory
2. Query Flooding
3. Exploiting Heterogeneity

1. Centralized Directory

A centralized Directory is somewhat similar to client-server architecture in the sense that it maintains a huge central server to provide directory service. All the peers inform this central server of their IP address and the files they are making available for sharing. The server queries the peers at regular intervals to make sure if the peers are still connected or not. So basically this server maintains a huge database regarding which file is present at which IP addresses. The first system which made use of this method was **Napster**, for Mp3 distribution.

Working

- Now whenever a requesting peer comes in, it sends its query to the server.
- Since the server has all the information of its peers, so it returns the IP addresses of all the peers having the requested file to the peer.
- Now the file transfer takes place between these two peers.


Bob
Inform & Update
1
Inform & Update
1
Peers
File Transfer
Centralized directory server
Inform & Update
1
3
Inform & Update
2
1
Alice
Query for content
P2P paradigm with a centralised directory

Centralized Directory

The major problem with such an architecture is that there is a single point of failure. If the server crashes, the whole P2P network crashes. Also, since all of the processing is to be done by a single server so a huge amount of the database has to be maintained and regularly updated.

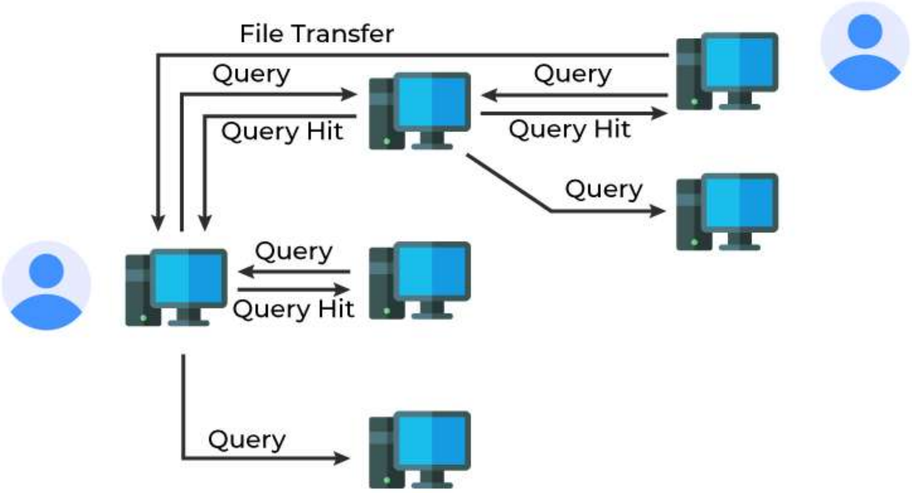
2. Query Flooding

Unlike the centralized approach, this method makes use of distributed systems. In this, the peers are supposed to be connected to an overlay network. It means if a connection/path exists from one peer to another, it is a part of this overlay network. In this overlay network, peers are called nodes, and the connection between peers is called an edge between the nodes, thus resulting in a graph-like structure. **Gnutella** was the first decentralized peer-to-peer network.

Working

- Now when one peer requests for some file, this request is sent to all its neighboring nodes i.e. to all nodes connected to this node. If those nodes don't have the required file, they pass on the query to their neighbors and so on. This is called query flooding.
- When the peer with the requested file is found (referred to as query hit), the query flooding stops and it sends back the file name and file size to the client, thus following the reverse path.
- If there are multiple query hits, the client selects from one of these peers.

Gnutella: Gnutella represents a new wave of P2P applications providing distributed discovery and sharing of resources across the Internet. Gnutella is distinguished by its support for anonymity and its decentralized architecture. A Gnutella network consists of a dynamically changing set of peers connected using TCP/IP.



Query Flooding

This method also has some disadvantages, the query has to be sent to all the neighboring peers unless a match is found. This increases traffic in the network.

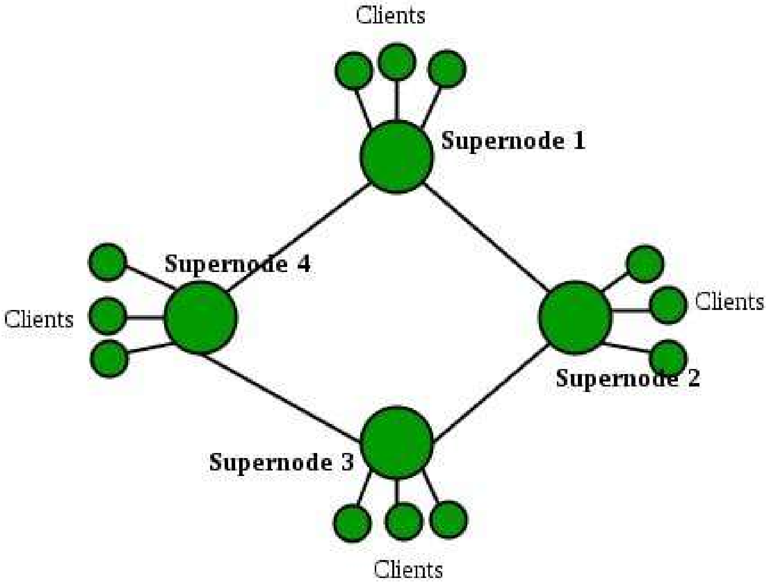
3. Exploiting Heterogeneity

This P2P architecture makes use of both the above-discussed systems. It resembles a distributed system like Gnutella because there is no central server for query processing. But unlike Gnutella, it does not treat all its peers equally. The peers with higher bandwidth and network connectivity are at a higher priority and are called **group leaders/supernodes**. The rest of the peers are assigned to these supernodes. These supernodes are interconnected and the peers under these supernodes inform their respective leaders about their connectivity, IP address, and the files available for sharing.

KaZaA technology is such an example that makes use of Napster and Gnutella. Thus, the individual group leaders along with their child peers form a Napster-like structure. These group leaders then interconnect among themselves to resemble a Gnutella-like structure.

Working

- This structure can process the queries in two ways.
- The first one is that the supernodes could contact other supernodes and merge their databases with their database. Thus, this supernode now has information about a large number of peers.
- Another approach is that when a query comes in, it is forwarded to the neighboring super nodes until a match is found, just like in Gnutella. Thus query flooding exists but with limited scope as each supernode has many child peers. Hence, such a system exploits the heterogeneity of the peers by designating some of them as group leaders/supernodes and others as their child peers



Exploiting heterogeneity

P2P File Sharing Security Concerns

Steps that ensure that Sensitive Information on the network is secure:

- You must delete your sensitive information which you don't require and you can apply some restrictions to important file present within the network.
- For strong or accessing sensitive information, try to reduce or remove P2P file-sharing programs on computers.
- Constantly try to monitor the network to find unauthorized file-sharing programs.
- Try to block the unauthorized Peer-to-Peer file sharing programs within the perimeter of the network.
- Implement strong access controls and authentication mechanisms to prevent unauthorized access to sensitive information on the network.
- Use encryption techniques such as Secure Socket Layer (SSL) or Transport Layer Security (TLS) to protect data in transit between peers on the network.
- Implement firewalls, intrusion detection and prevention systems, and other security measures to prevent unauthorized access to the network and to detect and block malicious activity.
- Regularly update software and security patches to address known vulnerabilities in P2P file-sharing programs and other software used on the network.

- Educate users about the risks associated with P2P file-sharing and provide training on how to use these programs safely and responsibly.
- Use data loss prevention tools to monitor and prevent the transmission of sensitive data outside of the network.
- Implement network segmentation to limit the scope of a security breach in case of a compromise, and to prevent unauthorized access to sensitive areas of the network.
- Regularly review and audit the network to identify potential security threats and to ensure that security controls are effective and up-to-date.

Comment More info Advertise with us

Next Article

P2P (Peer To Peer) File Sharing

Similar Reads

1. What is P2P (Peer-to-Peer Process)?
2. What is File server?
3. File Sharing App using Python
4. What is APPN(Advanced Peer to Peer Networking)
5. Introduction to Microsoft SMB; A network file sharing protocol
6. InterPlanetary File System
7. What is APPC(Advanced Peer to Peer Communication)?
8. What is TFTP (Trivial File Transfer Protocol)?
9. How to Share Files On Local Network Using Apache File Server?
10. Point-to-Point Protocol (PPP) Suite

Corporate & Communications Address:

Congestion Control in Computer Networks

Last Updated : 21 Feb, 2025

Congestion in a computer network happens when there is too much data being sent at the same time, causing the network to slow down. Just like traffic congestion on a busy road, network congestion leads to delays and sometimes data loss. When the network can't handle all the incoming data, it gets "clogged," making it difficult for information to travel smoothly from one place to another.

Congestion control is a crucial concept in computer networks. It refers to the methods used to prevent network overload and ensure smooth data flow.Congestion control techniques help manage the traffic, so all users can enjoy a stable and efficient network connection. These techniques are essential for maintaining the performance and reliability of modern networks.

Effects of Congestion Control

- **Improved Network Stability**: Congestion control helps keep the network stable by preventing it from getting overloaded. It manages the flow of data so the network doesn't crash or fail due to too much traffic.
- **Reduced Latency and Packet Loss**: Without congestion control, **data transmission** can slow down, causing delays and data loss. Congestion control helps manage traffic better, reducing these delays and ensuring fewer data packets are lost, making data transfer faster and the network more responsive.
- **Enhanced Throughput**: By avoiding congestion, the network can use its resources more effectively. This means more data can be sent in a shorter time, which is important for handling large amounts of data and supporting high-speed applications.

- **Fairness in Resource Allocation**: Congestion control ensures that network resources are shared fairly among users. No single user or application can take up all the bandwidth, allowing everyone to have a fair share.
- **Better User Experience**: When data flows smoothly and quickly, users have a better experience. Websites, online services, and applications work more reliably and without annoying delays.
- **Mitigation of Network Congestion Collapse**: Without congestion control, a sudden spike in data traffic can overwhelm the network, causing severe congestion and making it almost unusable. Congestion control helps prevent this by managing traffic efficiently and avoiding such critical breakdowns.

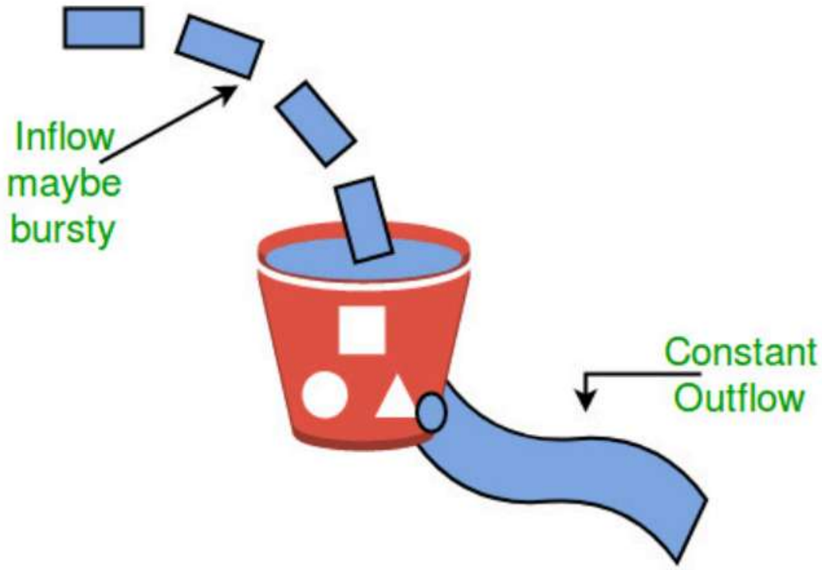
Congestion Control Algorithm

Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse. **Congestive-avoidance algorithms** (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.There are two congestion control algorithms which are as follows:

Leaky Bucket Algorithm

- The leaky bucket algorithm discovers its use in the context of network traffic shaping or rate-limiting.
- A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
- This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
- The disadvantages compared with the leaky-bucket algorithm are the inefficient use of available network resources.
- The large area of network resources such as bandwidth is not being used effectively.

Let us consider an example to understand. Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.



Leaky Bucket

Similarly, each network interface contains a leaky bucket and the following steps are involved in leaky bucket algorithm:

- When host wants to send packet, packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket.
- In practice the bucket is a finite queue that outputs at a finite rate.

Read in detail about **Leaky Bucket Algorithm**

Token Bucket Algorithm

- The leaky bucket algorithm has a rigid output design at an average rate independent of the bursty traffic.
- In some applications, when large bursts arrive, the output is allowed to speed up. This calls for a more flexible algorithm, preferably one that never loses information. Therefore, a token bucket algorithm finds its uses in network traffic shaping or rate-limiting.

- It is a control algorithm that indicates when traffic should be sent. This order comes based on the display of tokens in the bucket.
- The bucket contains tokens. Each of the tokens defines a packet of predetermined size. Tokens in the bucket are deleted for the ability to share a packet.
- When tokens are shown, a flow to transmit traffic appears in the display of tokens.
- No token means no flow sends its packets. Hence, a flow transfers traffic up to its peak burst rate in good tokens in the bucket.

Read in detail about **Token Bucket Algorithm**

Need of Token Bucket Algorithm

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

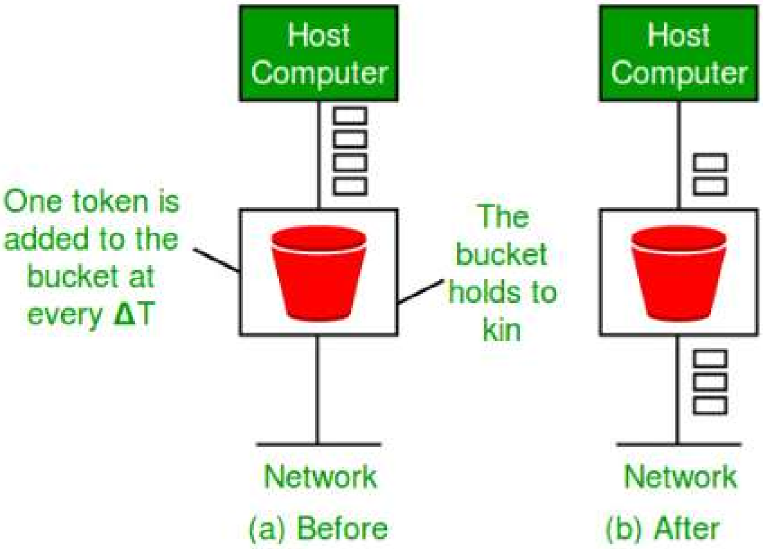
Steps of this algorithm can be described as follows:

- In regular intervals tokens are thrown into the bucket.
- The bucket has a maximum capacity.
- If there is a ready packet, a token is removed from the bucket, and the packet is sent.
- If there is no token in the bucket, the packet cannot be sent.

Let's understand with an example, In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

Token Bucket vs Leaky Bucket

The leaky bucket algorithm controls the rate at which the packets are introduced in the network, but it is very conservative in nature. Some flexibility is introduced in the token bucket algorithm. In the token bucket algorithm, tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.



Leaky Bucket

Advantages

- **Stable Network Operation**: Congestion control ensures that networks remain stable and operational by preventing them from becoming overloaded with too much data traffic.
- **Reduced Delays**: It minimizes delays in data transmission by managing traffic flow effectively, ensuring that data packets reach their destinations promptly.
- **Less Data Loss**: By regulating the amount of data in the network at any given time, congestion control reduces the likelihood of data packets being lost or discarded.
- **Optimal Resource Utilization**: It helps networks use their resources efficiently, allowing for better throughput and ensuring that users can access data and services without interruptions.
- **Scalability**: Congestion control mechanisms are scalable, allowing networks to handle increasing volumes of data traffic as they grow without compromising performance.

- **Adaptability**: Modern congestion control algorithms can adapt to changing network conditions, ensuring optimal performance even in dynamic and unpredictable environments.

Disadvantages

- **Complexity**: Implementing congestion control algorithms can add complexity to network management, requiring sophisticated systems and configurations.
- **Overhead**: Some congestion control techniques introduce additional overhead, which can consume network resources and affect overall performance.
- **Algorithm Sensitivity**: The effectiveness of congestion control algorithms can be sensitive to network conditions and configurations, requiring fine-tuning for optimal performance.
- **Resource Allocation Issues**: Fairness in resource allocation, while a benefit, can also pose challenges when trying to prioritize critical applications over less essential ones.
- **Dependency on Network Infrastructure**: Congestion control relies on the underlying network infrastructure and may be less effective in environments with outdated or unreliable equipment.

Comment More info Advertise with us

Next Article

Congestion Control techniques in Computer Networks

Similar Reads

1. Congestion Control techniques in Computer Networks
2. Congestion Control in Datagram Subnets
3. Delays in Computer Network
4. Functionality of Computer Network
5. TCP Congestion Control

TCP Congestion Control

Last Updated : 28 Dec, 2024

TCP congestion control is a method used by the TCP protocol to manage data flow over a network and prevent congestion. TCP uses a congestion window and congestion policy that avoids congestion. Previously, we assumed that only the receiver could dictate the sender's window size. We ignored another entity here, the network. If the network cannot deliver the data as fast as it is created by the sender, it must tell the sender to slow down. In other words, in addition to the receiver, the network is a second entity that determines the size of the sender's window.

Congestion Policy in TCP

- **Slow Start Phase:** Starts slow increment is exponential to the threshold.
- **Congestion Avoidance Phase:** After reaching the threshold increment is by 1.
- **Congestion Detection Phase:** The sender goes back to the Slow start phase or the Congestion avoidance phase.

Slow Start Phase

Exponential Increment: In this phase after every RTT the congestion window size increments exponentially.

Example: If the initial congestion window size is 1 segment, and the first segment is successfully acknowledged, the congestion window size becomes 2 segments. If the next transmission is also acknowledged, the congestion window size doubles to 4 segments. This exponential growth continues as long as all segments are successfully acknowledged.

```
Initially cwnd = 1
After 1 RTT, cwnd = 2^(1) = 2
2 RTT, cwnd = 2^(2) = 4
3 RTT, cwnd = 2^(3) = 8
```

Congestion Avoidance Phase

Additive Increment: This phase starts after the threshold value also denoted as **ssthresh.** The size of CWND (Congestion Window) increases additive. After each RTT cwnd = cwnd + 1.

For example: if the congestion window size is 20 segments and all 20 segments are successfully acknowledged within an RTT, the congestion window size would be increased to 21 segments in the next RTT. If all 21 segments are again successfully acknowledged, the congestion window size will be increased to 22 segments, and so on.

```
Initially cwnd = i
```

```
2 RTT, cwnd = i+2
3 RTT, cwnd = i+3
```

Congestion Detection Phase

Multiplicative Decrement: If congestion occurs, the congestion window size is decreased. The only way a sender can guess that congestion has happened is the need to retransmit a segment. Retransmission is needed to recover a missing packet that is assumed to have been dropped by a router due to congestion. Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received.

Case 1: Retransmission due to Timeout – In this case, the congestion possibility is high.

```
(a) ssthresh is reduced to half of the current window size.
(b) set cwnd = 1
```

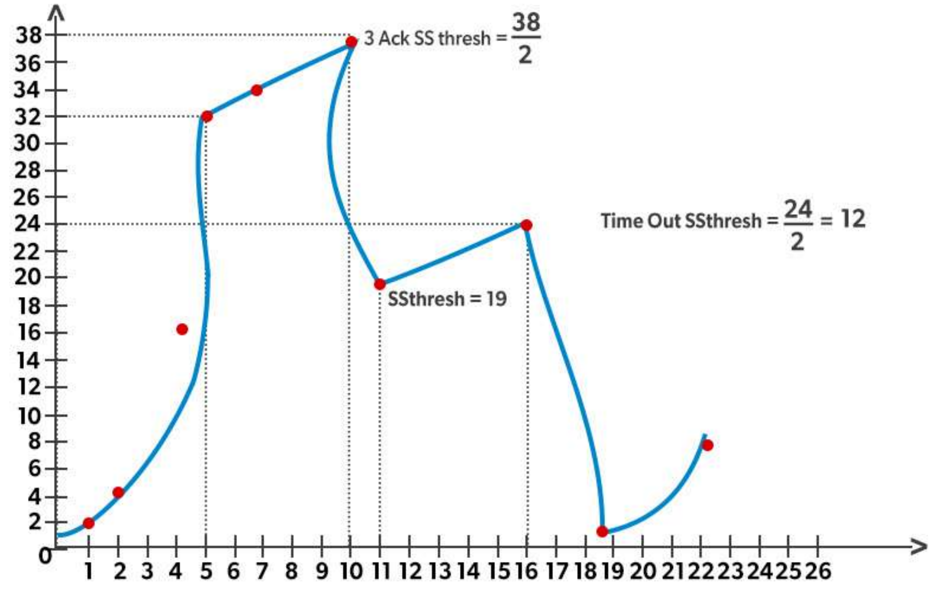
```
(c) start with the slow start phase again.
```

Case 2: Retransmission due to 3 Acknowledgement Duplicates – The congestion possibility is less.

```
(a) ssthresh value reduces to half of the current window size.
(b) set cwnd= ssthresh
(c) start with congestion avoidance phase
```

Example

Assume a [TCP protocol](#)experiencing the behavior of slow start. At the 5th transmission round with a threshold (ssthresh) value of 32 goes into the congestion avoidance phase and continues till the 10th transmission. At the 10th transmission round, 3 duplicate ACKs are received by the receiver and entered into additive increase mode. Timeout occurs at the 16th transmission round. Plot the transmission round (time) vs congestion window size of TCP segments.



Congestion Detection Phase

GATE CS Corner Questions

Practicing the following questions will help you test your knowledge. All questions have been asked in GATE in previous years or in GATE Mock Tests. It is highly recommended that you practice them.

1. GATE CS 2008, Question 56
2. GATE CS 2012, Question 65
3. GATE CS 2014 (Set 1), Question 65
4. GATE IT 2005, Question 73

Conclusion

In summary, TCP congestion control helps balance the data flow in a network, ensuring that all users can send and receive data efficiently without Overloading the network. It dynamically adjusts the data flow based on the network's current state, ensuring stable and reliable communication.

Comment More info Advertise with us

Next Article

Circuit Switching in Computer Network

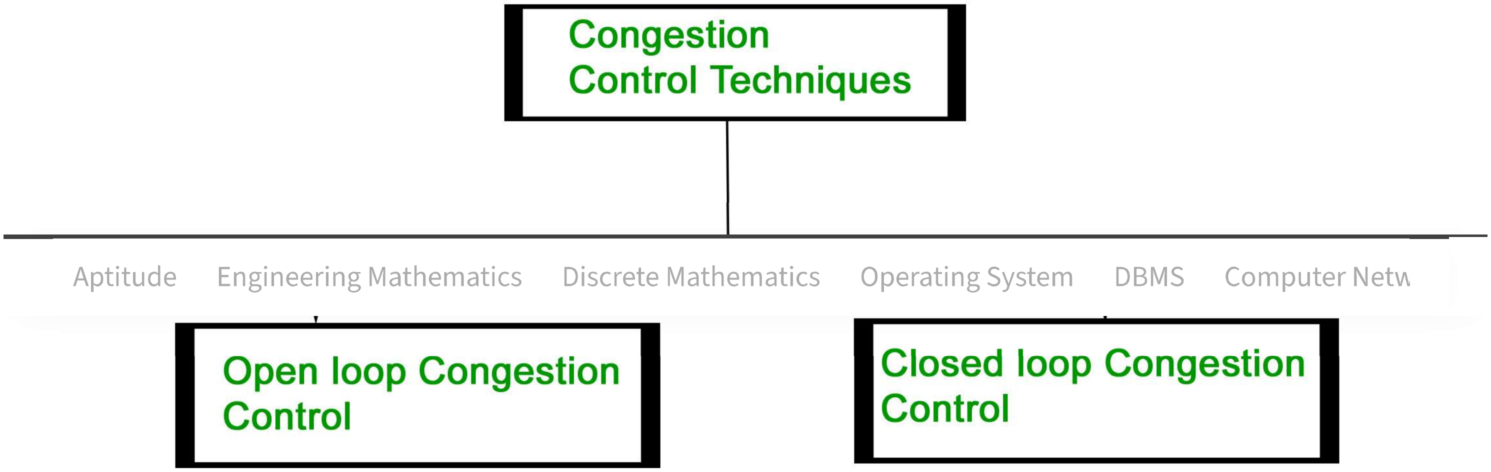
Similar Reads

1. Congestion Control in Datagram Subnets
2. Congestion Control in Computer Networks
3. What is DCCP (Datagram Congestion Control Protocol)?
4. Congestion Control techniques in Computer Networks
5. Error Control in TCP
6. TCP Congestion Control Algorithms: Reno, New Reno, BIC, CUBIC
7. Difference between Flow Control and Congestion Control
8. Slow Start Restart Algorithm For Congestion Control
9. TCP Connection Termination
10. Network Control Unit

Congestion Control techniques in Computer Networks

Last Updated : 28 Dec, 2024

Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:


Congestion Control Techniques
Open loop Congestion Control
Closed loop Congestion Control

Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control -

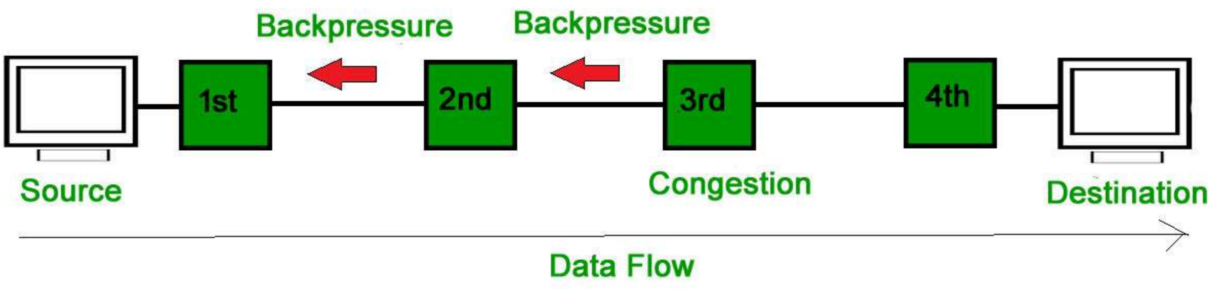
1. **Retransmission Policy :**
   It is the policy in which retransmission of the packets are taken care of. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.
   To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.
2. **Window Policy :**
   The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and make it worse.
   Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.
3. **Discarding Policy :**
   A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages and also be able to maintain the quality of a message.
   In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.
4. **Acknowledgment Policy :**
   Since acknowledgements are also the part of the load in the network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.
   The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send an acknowledgment only if it has to send a packet or a timer expires.

5. **Admission Policy :**
   In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

Closed Loop Congestion Control

Closed loop congestion control techniques are used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

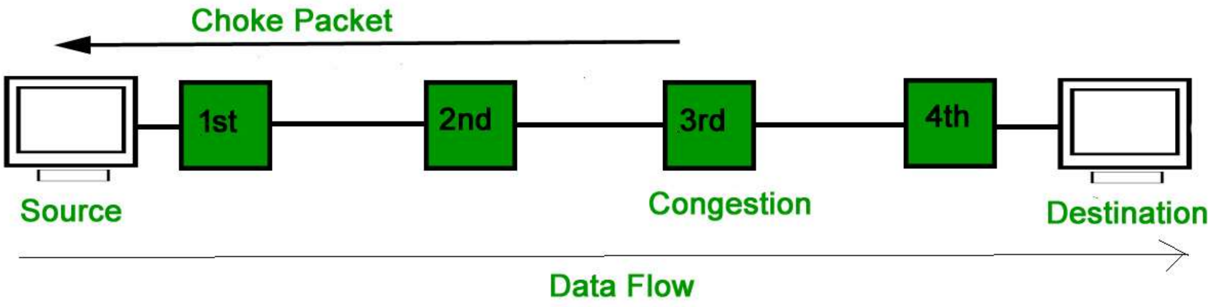
1. Backpressure :
Backpressure is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and reject receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.



In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and inform the source to slow down.

2. Choke Packet Technique :

Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.



3. Implicit Signaling :

In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

4. Explicit Signaling :

In explicit signaling, if a node experiences congestion it can explicitly send a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is

included in the packets that carry data rather than creating a different packet as in case of choke packet technique.
Explicit signaling can occur in either forward or backward direction.

- **Forward Signaling :** In forward signaling, a signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.
- **Backward Signaling :** In backward signaling, a signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

Comment More info Advertise with us

Next Article

Leaky bucket algorithm

Similar Reads

1. Congestion Control in Computer Networks
2. Error Correction in Computer Networks
3. Controlled Access Protocols in Computer Network
4. Types of Errors in Computer Network
5. Last Minute Notes for Computer Networks
6. TCP Congestion Control Algorithms: Reno, New Reno, BIC, CUBIC
7. Functionality of Computer Network
8. Congestion Control in Datagram Subnets
9. TCP Congestion Control
10. Delays in Computer Network

GeeksforGeeks
Sanchhaya Education Private Limited
Corporate & Communications Address:

Search...

53

Protocols in Application Layer

Last Updated : 28 Dec, 2024

The Application Layer is the topmost layer in the Open System Interconnection (OSI) model. This layer provides several ways for manipulating the data which enables any type of user to access the network with ease. The Application Layer interface directly interacts with the application and provides common web application services. The application layer performs several kinds of functions that are required in any kind of application or communication process. In this article, we will discuss various application layer protocols.

What are Application Layer Protocols?

Application layer protocols are those protocols utilized at the application layer of the OSI (Open Systems Interconnection) and TCP/IP models. They facilitate communication and data sharing between software applications on various network devices. These protocols define the rules

Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw

and effectively over a network.

Application Layer Protocol in Computer Network

1. TELNET

Telnet stands for the **TEL**etype **NET**work. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. It is used for managing files on the Internet. It is used for the initial setup of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. The port number of the telnet is 23.

Command

```
telnet [\\RemoteServer]
\\RemoteServer
: Specifies the name of the server
to which you want to connect
```

2. FTP

FTP stands for File Transfer Protocol. It is the protocol that actually lets us transfer files. It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP promotes sharing of files via remote computers with reliable and efficient data transfer. The Port number for FTP is 20 for data and 21 for control.

Command

```
ftp machinename
```

3. TFTP

The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it’s the protocol of choice if you know exactly what you want and where to find it. It's a technology for transferring files between network devices and is a simplified version of FTP. The Port number for TFTP is 69.

Command

```
tftp [ options... ] [host [port]] [-c command]
```

4. NFS

It stands for a Network File System. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network. The Port number for NFS is 2049.

Command

```
service nfs start
```

5. SMTP

It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. The Port number for SMTP is 25.

Command

```
MAIL FROM:<mail@abc.com?
```

6. LPD

It stands for Line Printer Daemon. It is designed for printer sharing. It is the part that receives and processes the request. A "daemon" is a server or agent. The Port number for LPD is 515.

Command

```
lpd [ -d ] [ -l ] [ -D DebugOutputFile]
```

7. X window

It defines a protocol for the writing of graphical user interface–based client/server applications. The idea is to allow a program, called a client, to run on one computer. It is primarily used in networks of interconnected mainframes. Port number for X window starts from 6000 and increases by 1 for each server.

Command

```
Run xdm in runlevel 5
```

8. SNMP

It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defined values. The Port number of SNMP is 161(TCP) and 162(UDP).

Command

```
snmpget -mALL -v1 -cpublic snmp_agent_Ip_address sysName.0
```

9. DNS

It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.abc.com might translate to 198.105.232.4.
The Port number for DNS is 53.

Command

```
ipconfig /flushdns
```

10. DHCP

It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.

Command

```
clear ip dhcp binding {address | * }
```

11. HTTP/HTTPS

HTTP stands for Hypertext Transfer Protocol and HTTPS is the more secured version of HTTP, that's why HTTPS stands for Hypertext Transfer Protocol Secure. This protocol is used to access data from the World Wide Web. The Hypertext is the well-organized documentation system that is used to link pages in the text document.

- HTTP is based on the client-server model.
- It uses TCP for establishing connections.
- HTTP is a stateless protocol, which means the server doesn't maintain any information about the previous request from the client.
- HTTP uses port number 80 for establishing the connection.

12. POP

POP stands for Post Office Protocol and the latest version is known as POP3 (Post Office Protocol version 3). This is a simple protocol used by User agents for message retrieval from mail servers.

- POP protocol work with Port number 110.
- It uses TCP for establishing connections.

POP works in dual mode- *Delete mode, Keep Mode*.

In Delete mode, it deletes the message from the mail server once they are downloaded to the local system.

In Keep mode, it doesn't delete the message from the mail server and also facilitates the users to access the mails later from the mail server.

13. IRC

IRC stands for Internet Relay Chat. It is a text-based instant messaging/chatting system. IRC is used for group or one-to-one communication. It also supports file, media, data sharing within the chat. It works upon the client-server model. Where users connect to IRC server or IRC network via some web/ standalone application program.

- It uses TCP or TLS for connection establishment.
- It makes use of port number 6667.

14. MIME

MIME stands for Multipurpose Internet Mail Extension. This protocol is designed to extend the capabilities of the existing Internet email protocol like SMTP. MIME allows non-ASCII data to be sent via SMTP. It allows users to send/receive various kinds of files over the Internet like audio, video, programs, etc. MIME is not a standalone protocol it works in collaboration with other protocols to extend their capabilities.

Conclusion

Application layer protocols are required to enable communication and data exchange between software applications on different network devices. These protocols, which include HTTP, FTP, SMTP, and DNS, specify the rules and standards that enable applications to communicate easily across a network. Each protocol serves a distinct purpose, ranging from file transfer and email management to network device configuration and web page access, providing efficient and effective network connection.

Comment More info Advertise with us

Next Article

Domain Name System (DNS)

Similar Reads

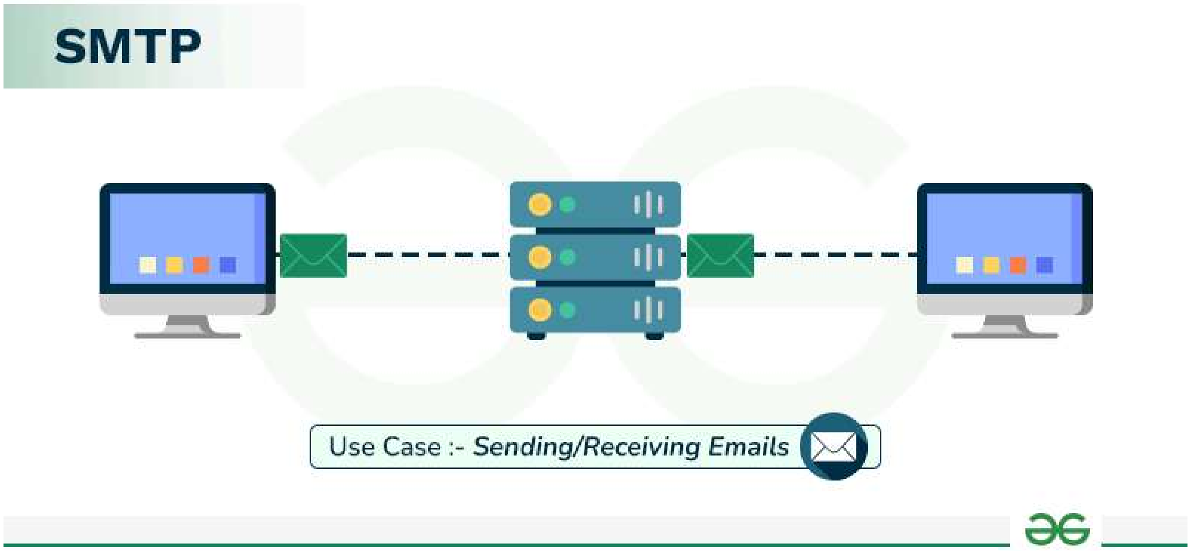
1. Application Layer Protocols in TCP/IP
2. Application Layer in OSI Model

Simple Mail Transfer Protocol (SMTP)

Last Updated : 14 May, 2025

Simple Mail Transfer Protocol (SMTP) is an application layer protocol used for exchanging email messages between servers. It is essential in the email communication process and operates at the application layer of the TCP/IP stack.

To send an email, the client opens a TCP connection to the SMTP server. The server, which is always listening on port 25, initiates the connection as soon as it detects a client. Once the TCP connection is established, the client sends the email across the connection.



SMTP

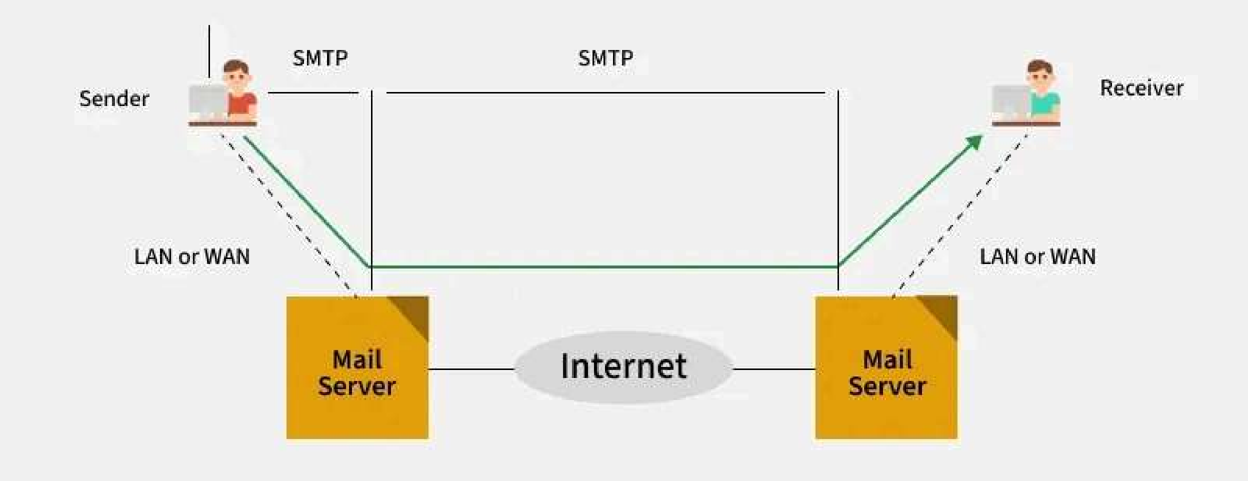
Types of SMTP Protocol

The **SMTP model** supports two types of email delivery methods: **end-to-end** and **store-and-forward**.

- **End-to-end** delivery is used between organizations. In this method, the email is sent directly from the sender's SMTP client to the recipient's SMTP server without passing through intermediate servers.

- **Store-and-forward** is used within organizations that have TCP/IP and SMTP-based networks. In this method, the email may pass through several intermediate servers (Message Transfer Agents, or MTAs) before reaching the recipient.

With **end-to-end** delivery, the SMTP client waits until the email is successfully copied to the recipient's SMTP server before sending it. This is different from the **store-and-forward** method, where the email might stop at multiple intermediate servers before reaching its destination. In store-and-forward systems, the sender is notified as soon as the email reaches the first server, not the final destination.



SMTP

Before diving deeper into the Model of SMTP System, it's important to understand how SMTP is leveraged by service providers like SMTP.com in the real-world scenario.

SMTP.com is a platform that caters to all your transaction, email relay and email delivery needs at a very affordable price. With decades of experience, SMTP.com is regarded as the most trusted sender in the industry by ISPs. SMTP.com had been trusted by over 100,000 customers over the years. SMTP.com is extremely intuitive and easy to set up. It can be integrated seamlessly into your current business system. If you need to migrate from another provider, SMTP.com make it effortless.

Features

- **Dedicated IP**
- Email API: Integrating SMTP.com with your business can be easy with the email API feature. They have complete API documentation on their website that can help you integrate your business in just 5 minutes.
- 24x7 Customer Support: The round-the-clock support is one of the best features of SMTP.com. Support is available both on the website and also for paid customers. 24x7, all human support is available for all customers across all plans. No third party is involved and solutions are provided fast for easy implementation. Online chat support is also available for those who are looking for more information about SMTP.com
- High Volume Sending Solutions: This newly launched feature is great for those businesses who want to send more than 250 million emails a month. Customized quotations and solutions are available.
- Reputation Defender: This is an add-on feature that helps clean up your email lists. It doesn't need any integration but actively monitors your lists and provides a report.

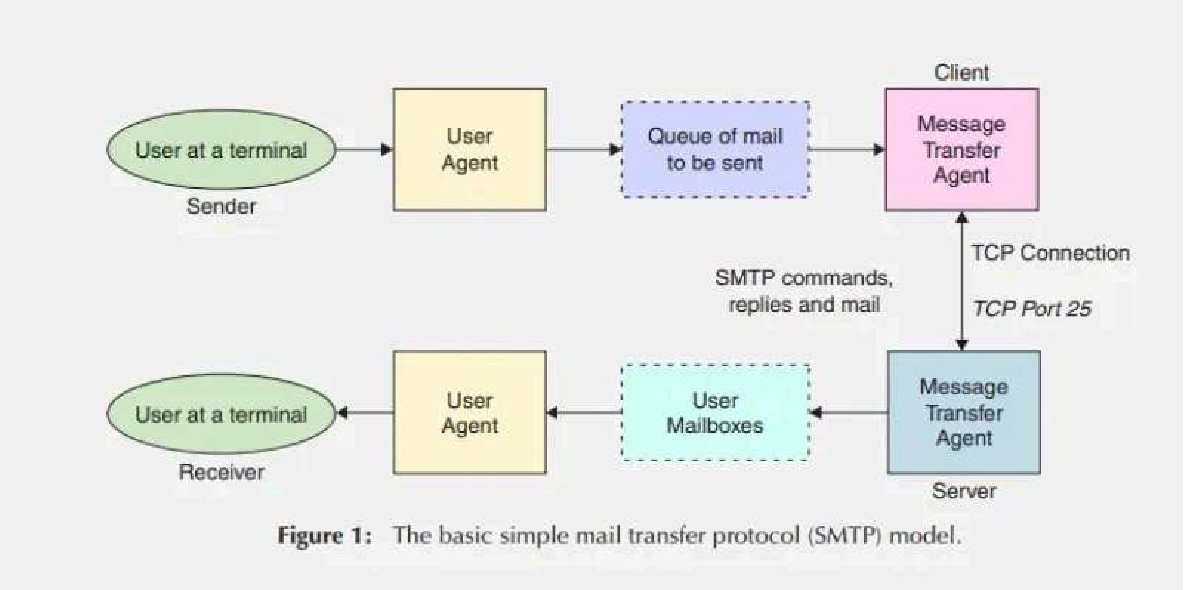
Pricing

SMTP.com offers affordable delivery services and caters to all kinds of

about this platform is that all the features are available in all the plans. The prices change only based on the volume of emails sent monthly. Even with the lowest price pack, users can get access to 24x7 customer support and all the SMTP tools. The Reputation Defender for list cleaning is an add-on feature available for all users.

Aptitude Engineering Mathematics Discrete Mathematics Operating System DBMS Computer Netw

Model of SMTP System


Client
User at a terminal
Sender
User Agent
Queue of mail to be sent
Message Transfer Agent
TCP Connection
SMTP commands, replies and mail
TCP Port 25
User at a terminal
Receiver
User Agent
User Mailboxes
Message Transfer Agent
Server
Figure 1: The basic simple mail transfer protocol (SMTP) model.

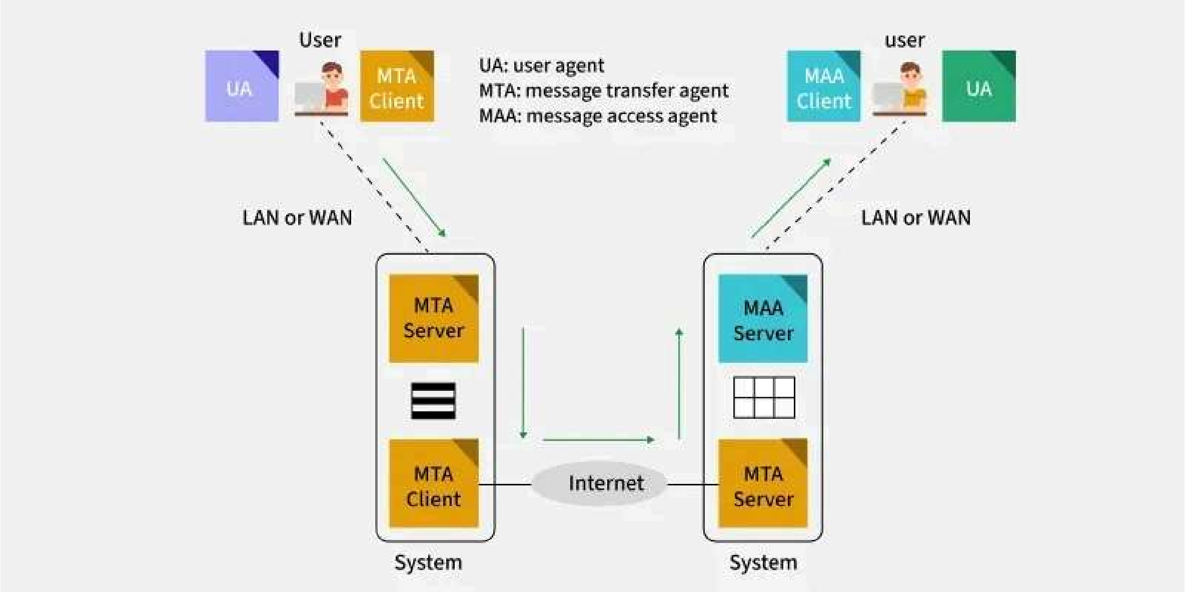
SMTP Model

In the SMTP model user deals with the user agent (UA), for example, Microsoft Outlook, Netscape, Mozilla, etc. To exchange the mail using TCP, MTA is used. The user sending the mail doesn't have to deal with MTA as it is the responsibility of the system admin to set up a local MTA. The MTA maintains a small queue of mail so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.

Components of SMTP

- **Mail User Agent (MUA):** It is a computer application that helps you in sending and retrieving mail. It is responsible for creating email messages for transfer to the mail transfer agent(MTA).
- **Mail Submission Agent (MSA):** It is a computer program that receives mail from a Mail User Agent(MUA) and interacts with the Mail Transfer Agent(MTA) for the transfer of the mail.
- **Mail Transfer Agent (MTA):** It is software that has the work to transfer mail from one system to another with the help of SMTP.
- **Mail Delivery Agent (MDA):** A mail Delivery agent or Local Delivery Agent is basically a system that helps in the delivery of mail to the local system.

How does SMTP Work?


User
UA
MTA Client
UA: user agent
MTA: message transfer agent
MAA: message access agent
user
MAA Client
UA
LAN or WAN
LAN or WAN
MTA Server
MAA Server
MTA Client
Internet
MTA Server
System
System

SMTP

1. Sending Email:

- When a user wants to send an email, they use a **User Agent (UA)**, like Outlook or Gmail.
- The email is handed over to the **MTA**, which is responsible for transferring the email to the recipient's mail server.

2. SMTP Client and Server:

- **Sender-SMTP (Client)**: The email sender's MTA initiates the connection to the recipient's MTA (Receiver-SMTP).
- **Receiver-SMTP (Server)**: The receiving MTA listens for incoming connections and receives the email from the sender-SMTP.
- This communication happens over TCP **port 25**.

3. Relays and Gateways:

- **Relays**: In some cases, the email may pass through several intermediate MTAs before reaching the destination server. These MTAs act as **relays**.
- **Gateways**: If the sending and receiving systems use different email protocols (e.g., SMTP and non-SMTP), an **email gateway** can convert the email to the appropriate format for delivery.

4. Email Delivery:

- The sender's **MTA** sends the email to the **receiver's MTA**, either directly or through relays.
- The **MTA** uses the **SMTP** protocol to transfer the message. Once it's delivered to the destination MTA, the email is placed in the recipient's mailbox.
- The recipient's **User Agent (UA)** can then download the email.

SMTP Envelope

Purpose

- The SMTP envelope contains information that guides email delivery between servers.
- It is distinct from the email headers and body and is not visible to the email recipient.

Contents of the SMTP Envelope

- **Sender Address**: Specifies where the email originates.
- **Recipient Addresses**: Indicates where the email should be delivered.
- **Routing Information**: Helps servers determine the path for email delivery.

Comparison to Regular Mail

- Think of the SMTP envelope as the **address on a physical envelope** for regular mail.
- Just like an envelope guides postal delivery, the SMTP envelope directs email servers on where to send the email.

SMTP Commands

S.No.	Keywor	Command form	Description	Usage
1.	HELO	HELO<SP><domain><CRLF>	It provides the identification of the sender i.e. the host name.	Mandatory
2.	MAIL	MAIL<SP>FROM : <reverse-path><CRLF>	It specifies the originator of the mail.	Mandatory
3.	RCPT	RCPT<SP>TO : <forward-path><CRLF>	It specifies the recipient of mail.	Mandatory
4.	DATA	DATA<CRLF>	It specifies the beginning of the mail.	Mandatory
5.	QUIT	QUIT<CRLF>	It closes the TCP connection.	Mandatory
6.	RSET	RSET<CRLF>	It aborts the current mail transaction but the TCP connection remains open.	Highly recommended
7.	VRFY	VRFY<SP><string><CRLF>	It is use to confirm or verify the user name.	Highly recommended

S.No.	Keywor	Command form	Description	Usage
8.	NOOP	NOOP<CRLF>	No operation	Highly recommended
9.	TURN	TURN<CRLF>	It reverses the role of sender and receiver.	Seldom used
10.	EXPN	EXPN<SP><string><CRLF>	It specifies the mailing list to be expanded.	Seldom used
11.	HELP	HELP<SP><string><CRLF>	It send some specific documentation to the system.	Seldom used
12.	SEND	SEND<SP>FROM : <reverse-path><CRLF>	It send mail to the terminal.	Seldom used
13.	SOML	SOML<SP>FROM : <reverse-path><CRLF>	It send mail to the terminal if possible; otherwise to mailbox.	Seldom used
14.	SAML	SAML<SP>FROM : <reverse-path><CRLF>	It send mail to the terminal and mailbox.	Seldom used

SMTP Ports

- **Port 587**: This is the most commonly used port for **secure SMTP submission** using **TLS (Transport Layer Security)**. It is recommended for client-to-server communication, as it ensures the security of the email transmission.
- **Port 465**: Previously used for **secure SMTP** (SMTPS), this port is **no longer considered an official standard** and is generally not recommended anymore. Many email providers have moved away from port 465 in favor of port 587.
- **Port 25**: This port is traditionally used for **SMTP relay** between mail servers, not for email submission from clients. It is often blocked by ISPs for outgoing mail due to its frequent use for spam and malicious activities.
- **Port 2525**: Although **not an official SMTP port**, it is sometimes used as an alternative for SMTP submission, especially in cases where port 25 is blocked or restricted. Many email providers support this port as an alternative for secure communication.

Difference Between SMTP and Extended SMTP

SMTP	Extended SMTP
Users were not verified in SMTP as a result of massive-scale scam emails being sent.	In Extended SMTP, authentication of the sender is done.
We cannot attach a Multimedia file in SMTP directly without the help of MMIE.	We can directly attach Multimedia FIle in ESMTP.
We cannot reduce the size of the email in SMTP.	We can reduce the size of the email in Extended SMTP.
SMTP clients open transmission with the command HELO.	The main identification feature for ESMTP clients is to open a

SMTP	Extended SMTP
	transmission with the command EHLO (Extended HELLO).

Advantages of SMTP

- If necessary, the users can have a dedicated server.
- It allows for bulk mailing.
- Low cost and wide coverage area.
- Offer choices for email tracking.
- Reliable and prompt email delivery.

Disadvantages of SMTP

- SMTP's common port can be blocked by several firewalls.
- SMTP security is a bigger problem.
- Its simplicity restricts how useful it can be.
- Just 7-bit ASCII characters can be used.
- If a message is longer than a certain length, SMTP servers may reject the entire message.
- Delivering your message will typically involve additional back-and-forth processing between servers, which will delay sending and raise the likelihood that it won't be sent.

SMTP vs POP vs IMAP

SMTP	POP	IMAP
Stands for Simple mail transfer protocol	Stands for Post Office Protocol.	Stands for Internet Message Access Protocol.

SMTP	POP	IMAP
Used for sending mail.	Used for retrieving mail.	Used for retrieving mail.
it is push protocol.	it is pull protocol.	it is pull protocol.
It work between sender's mail server to receiver's mail server and sender and sender's mail server.	It work between receiver and receiver's mail server.	It works between receiver and receiver's mail server.
It does not store mail on server it just send the mail.	It download all the mail when it connected to internet.	It store all mail on server and download when it get request to download.
Works on TCP port number 25.	Works on TCP port number 110.	Works on TCP port number 143.
Connection oriented protocol.	Connection oriented protocol.	Connection oriented protocol.
It has persistence TCP connection.	It has persistence TCP connection.	It has persistence TCP connection.
Stateless protocol.	Stateful protocol.	Stateful protocol.
It is in band protocol.	It is in band protocol.	It is in band protocol.

SMTP	POP	IMAP
Not used at receiver side.	Used at receiver side.	Used at receiver side.

Comment More info Advertise with us

Next Article

Introduction to TELNET

Similar Reads

1. SFTP File Transfer Protocol
2. What is ESMTP (Extended Simple Mail Transfer Protocol)?
3. XMODEM File Transfer Protocol
4. Transport Layer Protocols
5. What is TFTP (Trivial File Transfer Protocol)?
6. Stream Control Transmission Protocol (SCTP)
7. Email Protocols
8. Basics of SOAP - Simple Object Access Protocol
9. HTTP Full Form - Hypertext Transfer Protocol
10. File Transfer Protocol (FTP) in Application Layer

Domain Name System (DNS)

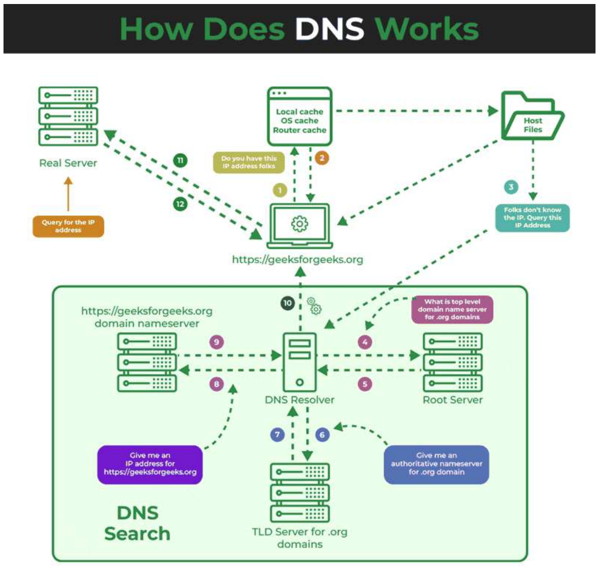
Last Updated : 09 Jun, 2025

DNS is a **hierarchical and distributed naming system** that translates domain names into IP addresses. When you type a domain name like `www.geeksforgeeks.org` into your browser, DNS ensures that the request reaches the correct server by resolving the domain to its corresponding IP address.

Without DNS, we'd have to remember the numerical IP address of every website we want to visit, which is highly impractical. DNS simplifies the process by allowing us to use user-friendly names while still maintaining the performance and scalability required for modern internet operations.

How Does DNS Work?

The DNS process can be broken down into several steps, ensuring that users can access websites by simply typing a domain name into their browser.


How Does DNS Works
Real Server
Query for the IP address
Local cache OS cache Router cache
Do you have this IP address folks
Host Files
Folks don't know the IP. Query this IP Address
https://geeksforgeeks.org
1
2
3
4
5
6
7
8
9
10
11
12
https://geeksforgeeks.org domain nameserver
DNS Resolver
Root Server
What is top level domain name server for .org domains
Give me an IP address for https://geeksforgeeks.org
Give me an authoritative nameserver for .org domain
TLD Server for .org domains
DNS Search

1. **User Input**: You enter a website address (for example, `www.geeksforgeeks.org`) into your web browser.

2. **Local Cache Check**: Your browser first checks its local cache to see if it has recently looked up the domain. If it finds the corresponding IP address, it uses that directly without querying external servers.
3. **DNS Resolver Query**: If the IP address isn't in the local cache, your computer sends a request to a DNS resolver. The resolver is typically provided by your Internet Service Provider (ISP) or your network settings.
4. **Root DNS Server**: The resolver sends the request to a root DNS server. The root server doesn't know the exact IP address for `www.geeksforgeeks.org` but knows which Top-Level Domain (TLD) server to query based on the domain's extension (e.g., `.org`).
5. **TLD Server**: The TLD server for `.org` directs the resolver to the authoritative DNS server for `geeksforgeeks.org`.
6. **Authoritative DNS Server**: This server holds the actual DNS records for `geeksforgeeks.org`, including the IP address of the website's server. It sends this IP address back to the resolver.
7. **Final Response**: The DNS resolver sends the IP address to your computer, allowing it to connect to the website's server and load the page.

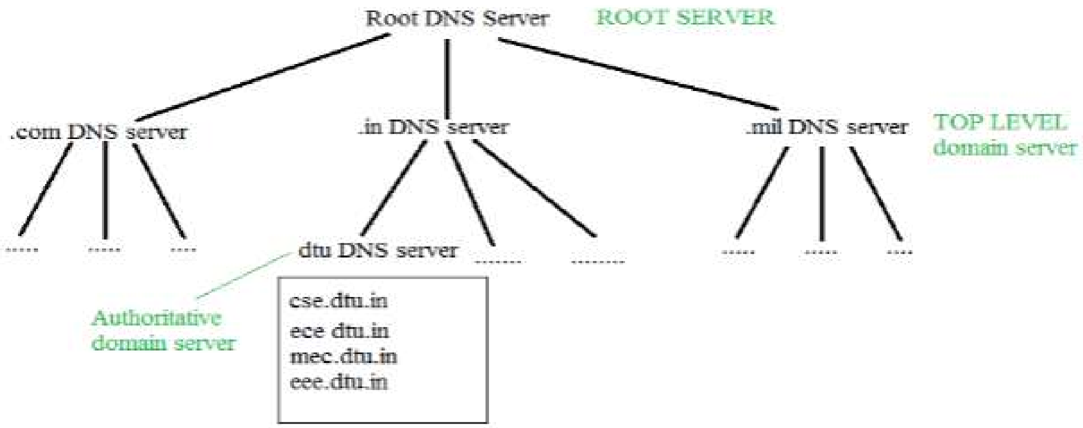
Note: This entire process happens in milliseconds, enabling a fast and efficient browsing experience.

Structure of DNS

DNS operates through a hierarchical structure, ensuring scalability and reliability across the global internet infrastructure. Here's how it's organized:

- **Root DNS Servers**: These are the highest-level DNS servers and know where to find the TLD servers. They are crucial for directing DNS queries to the correct locations.
- **TLD Servers**: These servers manage domain extensions like `.com`, `.org`, `.net`, `.edu`, `.gov`, and others. They help route queries to the authoritative DNS servers for specific domains.

- **Authoritative DNS Servers**: These are the servers that store the actual DNS records for domain names. They are responsible for providing the correct IP addresses that allow users to reach websites.


Root DNS Server
ROOT SERVER
.com DNS server
.in DNS server
.mil DNS server
TOP LEVEL domain server
dtu DNS server
Authoritative domain server
cse.dtu.in
ece dtu.in
mec.dtu.in
eee.dtu.in

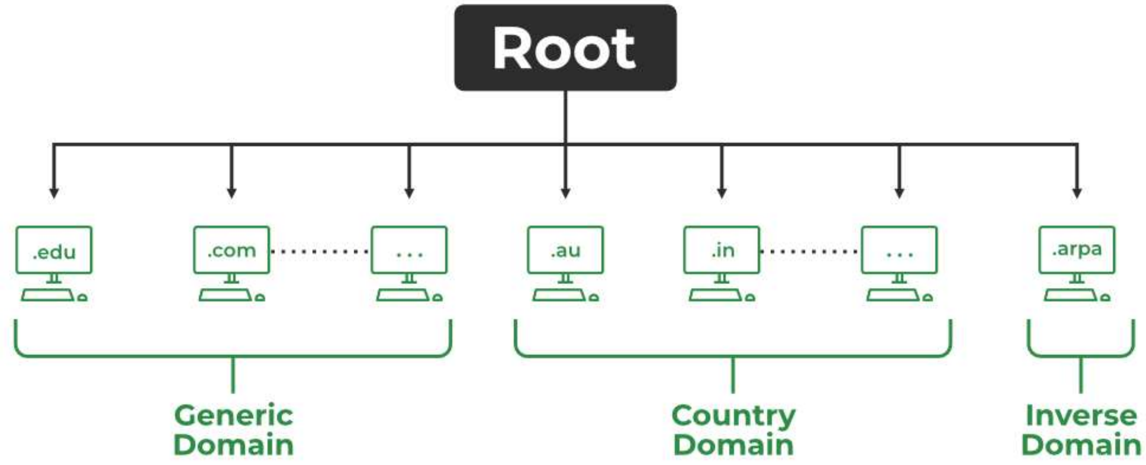
This hierarchical approach allows DNS to handle billions of queries every day, ensuring the stability and scalability of the internet.

Types of Domains

DNS helps manage a wide variety of domain types to organize the vast number of websites on the internet. Here are the primary categories:

- **Generic Domains**: These include top-level domains like `.com`, `.org`, `.net`, and `.edu`. These are widely used and recognized across the world.
- **Country Code Domains**: These domains represent specific countries or regions, such as `.in` for India, `.us` for the United States, `.uk` for the United Kingdom, and `.jp` for Japan.
- **Inverse Domains**: Used for reverse DNS lookups, these domains help map IP addresses back to domain names. Reverse DNS lookups are useful for diagnostics and security purposes, ensuring that the source of network traffic is legitimate. So DNS can provide both the mapping for example to find the IP addresses of geeksforgeeks.org then we have to type

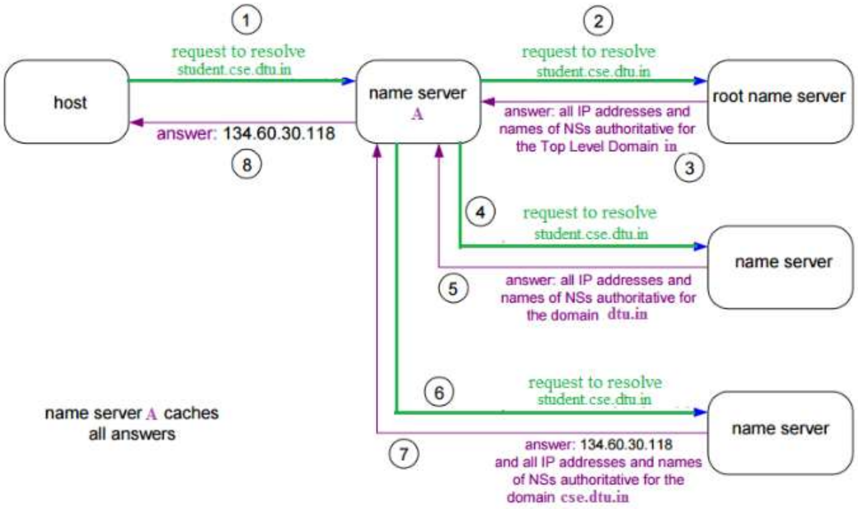
```
nslookup www.geeksforgeeks.org
```



Understanding these categories is essential for managing domains effectively and recognizing the purpose behind different types of domains.

Domain Name Server

The client machine sends a request to the local name server, which, if the root does not find the address in its database, sends a request to the root name server, which in turn, will route the query to a top-level domain (TLD) or authoritative name server. The root name server can also contain some **hostName** to IP address mappings. The Top-level domain (TLD) server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.


①
request to resolve student.cse.dtu.in
②
request to resolve student.cse.dtu.in
host
name server A
root name server
answer: 134.60.30.118
⑧
answer: all IP addresses and names of NSs authoritative for the Top Level Domain in
③
④
request to resolve student.cse.dtu.in
name server
⑤
answer: all IP addresses and names of NSs authoritative for the domain dtu.in
⑥
request to resolve student.cse.dtu.in
name server
name server A caches all answers
⑦
answer: 134.60.30.118 and all IP addresses and names of NSs authoritative for the domain cse.dtu.in

Domain Name Server

DNS Lookup

DNS Lookup, also called DNS Resolution, is the process of translating a human-readable domain name (like www.example.com) into its corresponding IP address (like 192.0.2.1), which computers use to locate and communicate with each other on the internet. It allows users to access websites easily using names instead of remembering numeric IP addresses.

- DNS Lookup starts when a user types a domain name into their browser.
- The query goes through a series of servers: the DNS resolver, Root server, TLD server, and authoritative server.
- Each server plays a role in finding the correct IP address for the domain.
- Once the IP address is found, the browser connects to the website's server and loads the page.

DNS Resolver

DNS Resolver is simply called a DNS Client and has the functionality for initiating the process of DNS Lookup which is also called DNS Resolution. By using the DNS Resolver, applications can easily access different websites and services present on the Internet by using domain names that are very much friendly to the user and that also resolves the problem of remembering IP Address.

Types of DNS Queries

There are basically three types of DNS Queries that occur in DNS Lookup. These are stated below.

- **Recursive Query:** In this query, if the resolver is unable to find the record, in that case, DNS client wants the DNS Server will respond to the client in any way like with the requested source record or an error message.
- **Iterative Query:** Iterative Query is the query in which DNS Client wants the best answer possible from the DNS Server.
- **Non-Recursive Query:** Non-Recursive Query is the query that occurs when a DNS Resolver queries a DNS Server for some record that has access to it because of the record that exists in its cache.

DNS Caching and TTL (Time-to-Live)

DNS caching is a mechanism that stores DNS records locally to avoid querying external DNS servers repeatedly for the same information. This speeds up the browsing experience and reduces network traffic.

TTL (Time-to-Live) is the amount of time that a DNS record is cached before it expires. When the TTL expires, the cache is cleared, and a fresh DNS query must be made. The TTL is defined by the authoritative DNS server, which can adjust this based on the nature of the domain.

For example, if the TTL for `www.geeksforgeeks.org` is set to 3600 seconds (1 hour), then the DNS record will be stored in the cache for one hour before it expires and requires a new lookup.

By understanding how DNS caching and TTL work, students can learn how to optimize website performance and troubleshoot issues related to stale or outdated DNS records.

DNS Security and DNSSEC (DNS Security Extensions)

Although DNS is essential for smooth internet navigation, it can be vulnerable to security threats. One common risk is **DNS cache poisoning**, where malicious actors inject harmful DNS records into caches, redirecting users to fraudulent websites.

DNS Security Extensions (DNSSEC) is a protocol designed to address these security concerns. It adds cryptographic signatures to DNS records, allowing resolvers to verify the authenticity and integrity of DNS responses. DNSSEC ensures that the information a user receives from a DNS query has not been tampered with.

By understanding DNSSEC, students can help secure websites against DNS-based attacks, ensuring safe and authentic browsing experiences.

Reverse DNS Lookup

Reverse DNS Lookup is the process of mapping an IP address back to its corresponding domain name. This is the opposite of the typical DNS lookup, where a domain name is resolved to an IP address. Reverse DNS is commonly used for:

- **Network Diagnostics**: System administrators use reverse DNS to determine the domain name associated with a specific IP address. This helps identify the source of network traffic.
- **Email Security**: Many email servers perform reverse DNS lookups to verify that incoming emails are coming from legitimate sources. This helps prevent spam and fraud.

A reverse DNS lookup is typically used in conjunction with standard DNS to ensure a complete and accurate mapping of network resources.

DNS Record Types (A, CNAME, MX, TXT, etc.)

DNS records are essential for defining how domain names are used and how services are configured. Here are some of the most commonly used DNS record types:

- **A Record**: This record maps a domain name to an IPv4 address (e.g., `geeksforgeeks.org` to `185.199.109.153`). This is the most common DNS record used to point a domain to its website's IP address.
- **CNAME Record**: The Canonical Name (CNAME) record allows you to alias one domain name to another. For example, `www.geeksforgeeks.org` can be an alias for `geeksforgeeks.org`.
- **MX Record**: The Mail Exchange (MX) record defines which mail servers are responsible for receiving emails for a domain. This is crucial for setting up email services.
- **TXT Record**: The Text (TXT) record stores text-based information. It is commonly used to verify domain ownership and to implement email security protocols like SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail).

By understanding these record types, students can gain the knowledge needed to configure web and email services, troubleshoot issues, and enhance their web development skills.

Comment More info

Campus Training Program

Next Article

Records in DNS

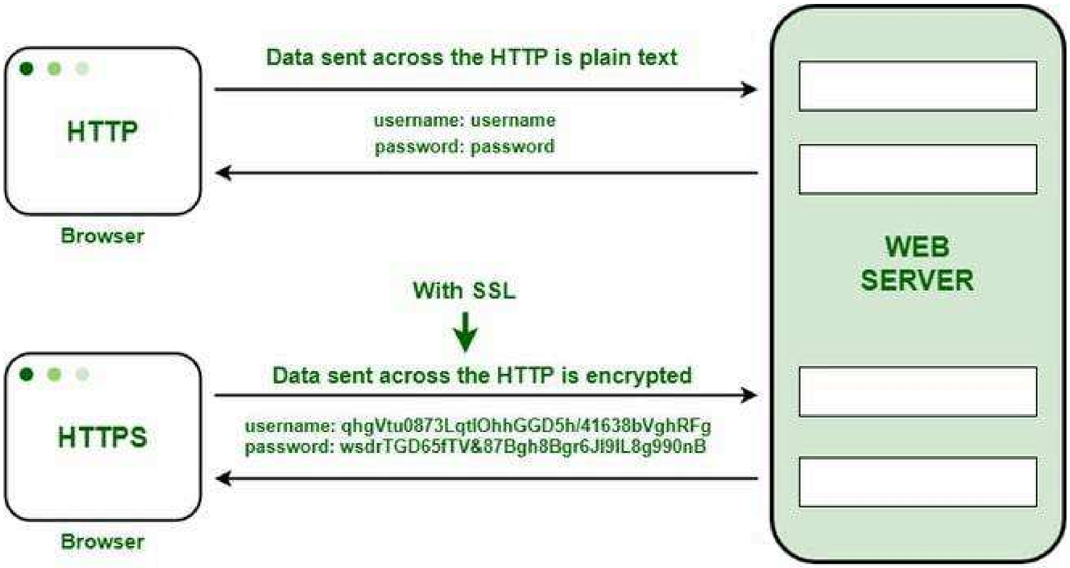
Similar Reads

1. Domain Name System (DNS) Zones
2. Working of Domain Name System (DNS) Server
3. DNS Message Format
4. How to Register a Domain Name ?
5. Dynamic Domain Name System (DDNS) in Application Layer
6. What is Domain Name System Security Extensions (DNSSEC)?
7. Address Resolution in DNS (Domain Name Server)
8. Difference Between Trademark and Domain Name
9. Introduction to Domain Name

Difference between http:// and https://

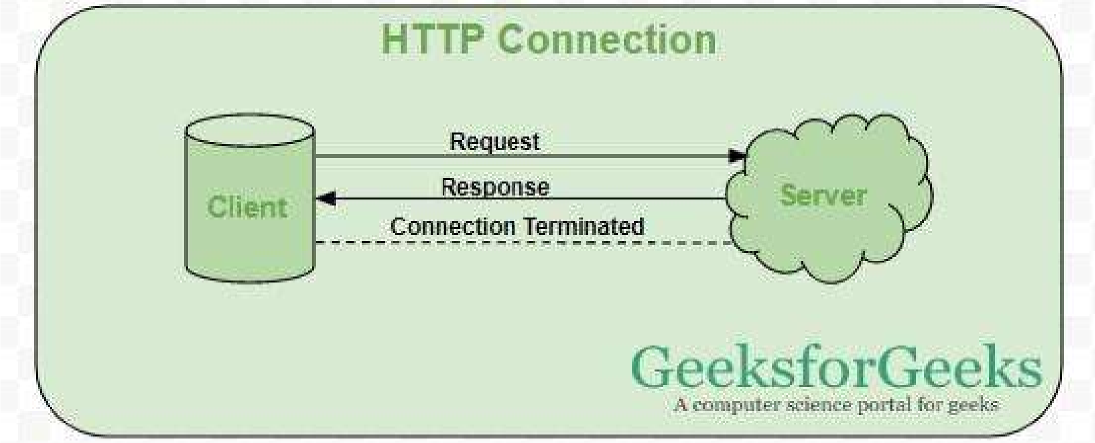
Last Updated : 26 Nov, 2024

When browsing the web, you might have noticed URLs starting with http. It is either 'http://' or 'https://'. Such prefixes show how data is transmitted between your browser and the website that you are accessing. HTTP and HTTPS are both protocols for communication but they are different in several ways and the main difference is security. This article will define HTTP and HTTPS as well as their features and why HTTPS is more frequently used than HTTP.


HTTP
Browser
Data sent across the HTTP is plain text
username: username
password: password
With SSL
HTTPS
Browser
Data sent across the HTTP is encrypted
username: qhgVtu0873LqtlOhhGGD5h/41638bVghRFg
password: wsdrTGD65fTV&87Bgh8Bgr6JI9IL8g990nB
WEB
SERVER

What is HTTP?

HTTP stands for HyperText Transfer Protocol. It is invented by Tim Berner. HyperText is the type of text that is specially coded with the help of some standard coding language called HyperText Markup Language (HTML). HTTP provides a standard between a web browser and a web server to establish communication. It is a set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, the user indirectly uses HTTP. It is an application protocol that is used for distributed, collaborative, hypermedia information systems.


HTTP Connection
Client
Request
Response
Connection Terminated
Server
GeeksforGeeks
A computer science portal for geeks

HTTP

Characteristics of HTTP

- HTTP is IP based communication protocol that is used to deliver data from server to client or vice-versa.
- Any type of content can be exchanged as long as the server and client are compatible with it.
- It is a request and response protocol based on client and server requirements.

HTTP Request

HTTP request is a kind of message a client (in most cases, a web browser) sends to the server demanding some specific resources. It comprises of several elements like the request method (GET, POST and etc.), the headers and occasionally the body carrying the data. This is the request part where the client outlines a request to the server and what they want.

HTTP Response

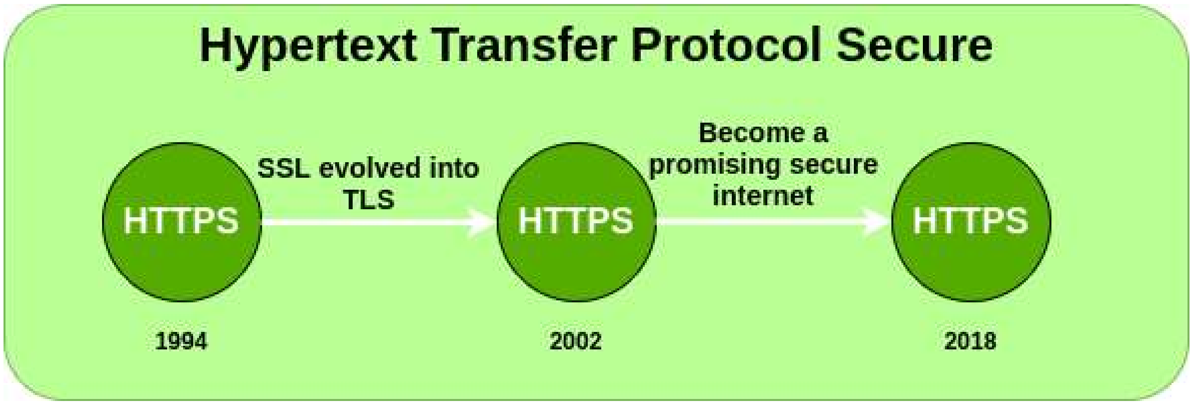
Http response is a message sent by the server to the client in response to an Http request. In simple terms, it has status code that describes the result of a request; header, which is information about the response; and the body, which is the actual response or an error message.

How Does the HTTP Protocol Work?

This means that the HTTP protocol uses a forms of a request and response operational mode. When a client wants to retrieve information, it uses http request to the servers as shown in the following stages. The request is received by the server and in the form of an HTTP response the server returns the data which the client requested or an error message. This takes place over the internet using port 80 by default, to assist in the identification of this protocol it is often referred to as the http or the hip protocol.

What is HTTPS?

HTTPS stands for Hyper Text Transfer Protocol Secure. HTTP Secure (HTTPS), could be a combination of the Hypertext Transfer Protocol with the SSL/TLS convention to supply encrypted communication and secure distinguishing proof of an arranged web server. HTTPS is more secure than HTTP because HTTPS is certified by the SSL(Secure Socket Layer). Whatever website you are visiting on the internet, if its URL is HTTP, then that website is not secure.


Hypertext Transfer Protocol Secure
HTTPS
SSL evolved into TLS
HTTPS
Become a promising secure internet
HTTPS
1994
2002
2018

HTTPS

Characteristics of HTTPS

- HTTPS encrypts all message substance, including the HTTP headers and the request/response data. The verification perspective of HTTPS requires a trusted third party to sign server-side digital certificates.
- HTTPS is presently utilized more frequently by web clients than the first non-secure HTTP, fundamentally to ensure page genuineness on all sorts of websites, secure accounts and to keep client communications.

In short, both of these are protocols using which the information of a particular website is exchanged between the Web Server and Web Browser. But there are some differences between these two. A concise difference between HTTP and HTTPS is that HTTPS is much more secure compared to HTTP.

How Does the HTTPS Protocol Work?

HTTPS can be said to be similar to the HTTP only that it also provides a level of security. It first creates a connection between the client and server over SSL/TLS, which enhances security by encrypting the Client and server communication. When a client makes a request for a resource using the https then the server and the client agree on the encryption keys that will be used in encrypting the data that will be transmitted in that particular session. This makes sure that data being exchanged between them is encrypted and coded hence cannot be intercepted.

Difference Between HTTP and HTTPS

HTTP	HTTPS
HTTP stands for HyperText Transfer Protocol. In HTTP, the URL begins with “http://”.	HTTPS stands for HyperText Transfer Protocol Secure. In HTTPS, the URL starts with “https://”.

HTTP	HTTPS
HTTP uses port number 80 for communication.	HTTPS uses port number 443 for communication.
Hyper-text exchanged using HTTP goes as plain text i.e. anyone between the browser and server can read it relatively easily if one intercepts this exchange of data and due to which it is Insecure.	HTTPS is considered to be secure but at the cost of processing time because Web Server and Web Browser need to exchange encryption keys using Certificates before actual data can be transferred.
HTTP Works at the Application Layer.	HTTPS works at Transport Layer.
HTTP does not use encryption, which results in low security in comparison to HTTPS.	HTTPS uses Encryption which results in better security than HTTP.
HTTP speed is faster than HTTPS.	HTTPS speed is slower than HTTP.
HTTP does not use data hashtags to secure data.	HTTPS will have the data before sending it and returning it to its original state on the receiver side.
HTTP is used to transfer text, video, and images via web pages.	HTTPS is used to transfer data securely via a network.

Hypertext Transfer Protocol (HTTP) is a protocol using which hypertext is transferred over the Web. Due to its simplicity, HTTP has been the most widely used protocol for data transfer over the Web but the data (i.e. hypertext) exchanged using HTTP isn’t as secure as we would like it to be. Cryptographic protocols such as SSL and/or TLS turn HTTP into HTTPS i.e. **HTTPS = HTTP + Cryptographic Protocols**.

Conclusion

HTTP and HTTPS are protocols that are used in the web to transfer data. HTTPS is more secure since it is encrypted and authenticated. HTTP is recommended for use in delivering non-sensitive information and is adequate for this job, while HTTPS is important in securing online transactions and the information of the user. With the emergence of new technologies the usage of the HTTPS protocol is expected to be the standard for secure browsing.

Comment More info Advertise with us

Next Article

Difference between http:// and https://

Similar Reads

1. Difference Between HTTP and HTTPS
2. Difference between FTP and HTTP
3. Difference between HTML and HTTP
4. Difference Between SMTP and HTTP
5. Difference between HTTP and IPFS
6. Difference between SOAP and HTTP
7. Difference between MQTT and HTTP protocols
8. Difference between SSH and SSL
9. Difference between HTTP GET and POST Methods
10. Difference between AMQP and HTTP Protocols

Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh

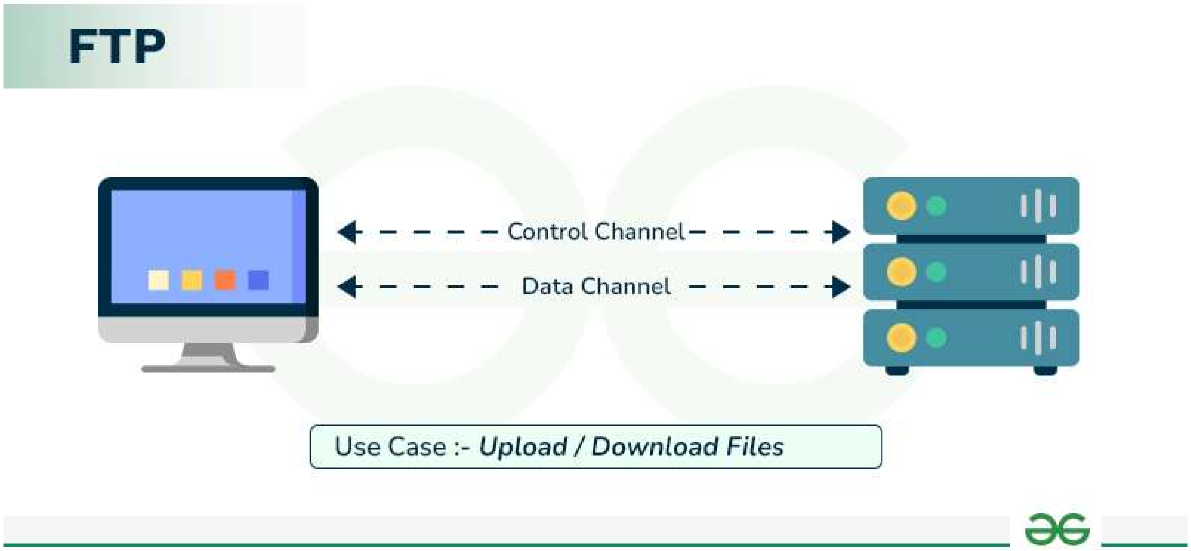
File Transfer Protocol (FTP) in Application Layer

Last Updated : 28 Dec, 2024

FTP or File Transfer Protocol is said to be one of the earliest and also the most common forms of transferring files on the internet. Located in the application layer of the OSI model, FTP is a basic system that helps in transferring files between a client and a server. It is what makes the FTP unique that the system provides a reliable and efficient means of transferring files from one system to another even if they have different file structures and operating systems. Contrary to other protocols such as http that cover hypertexts and web resources in general, ftp is dedicated to the management and the transfer of text, binary, or image files.

What is File Transfer Protocol?

FTP is a standard communication protocol. There are various other protocols like HTTP which are used to transfer files between computers, but they lack clarity and focus as compared to FTP. Moreover, the systems involved in connection are heterogeneous, i.e. they differ in operating systems, directories, structures, character sets, etc the FTP shields the user from these differences and transfers data efficiently and reliably. FTP can transfer ASCII, EBCDIC, or image files. The ASCII is the default file share format, in this, each character is encoded by NVT ASCII. In ASCII or EBCDIC the destination must be ready to accept files in this mode. The image file format is the default format for transforming binary files.



File Transfer Protocol

The **File Transfer Protocol (FTP)** is widely used in the application layer of networking. It works at the application layer, ensuring that files are sent and received securely.

Types of FTP

There are different ways through which a server and a client do a file transfer using FTP. Some of them are mentioned below:

- **Anonymous FTP:** Anonymous FTP is enabled on some sites whose files are available for public access. A user can access these files without having any username or password. Instead, the username is set to anonymous, and the password is to the guest by default. Here, user access is very limited. For example, the user can be allowed to copy the files but not to navigate through directories.

- **Password Protected FTP:** This type of FTP is similar to the previous one, but the change in it is the use of username and password.

- **FTP Secure (FTPS):** It is also called as FTP Secure Sockets Layer (FTP SSL). It is a more secure version of FTP data transfer. Whenever FTP connection is established, Transport Layer Security (TLS) is enabled.

- **FTP over Explicit SSL/TLS (FTPES):** FTPES helps by upgrading FTP Connection from port 21 to an encrypted connection.

- **Secure FTP (SFTP):** SFTP is not a FTP Protocol, but it is a subset of Secure Shell Protocol, as it works on port 22.

What is FTP Useful For?

FTP is especially useful for:

- **Transferring Large Files:** FTP can transfer large files in one shot; thus applicable when hosting websites, backing up servers, or sharing files in large quantities.
- **Remote File Management:** Files on a remote server can be uploaded, downloaded, deleted, renamed, and copied according to the users' choices.
- **Automating File Transfers:** FTP is a great protocol for the execution of file transfers on predefined scripts and employments.
- **Accessing Public Files:** Anonymous FTP means that everybody irrespective of the identity is allowed to download some files with no permissions needed.

How to Use FTP?

To use FTP, follow these steps:

- **Connect to the FTP Server:** One can connect to the server using the address, username and password through an FTP client or a command line interface. Anonymous Information may not need a username and password.
- **Navigate Directories:** Some commands include ls that is used to list directories and cd that is used to change directories.
- **Transfer Files:** File transfer may be done by using the commands such as get for downloading files, and put for uploading files.
- **Manage Files:** Make operations like deletion (Delete), renaming (Rename) as well as copying (Copy) of files.
- **Close the Connection:** Once file transfer has been accomplished, terminate the connection by giving the bye or quit command.

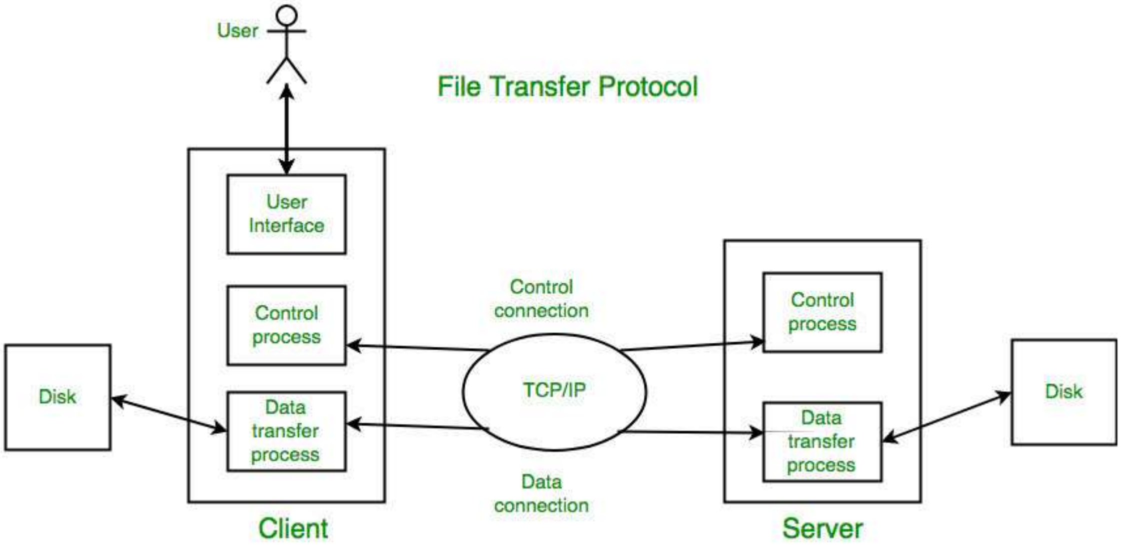
How Does FTP Work?

FTP is a client server protocol that has two communication channel, command channel for conversation control and data channel for file content.

Here are steps mentioned in which FTP works:

- A user has to log in to FTP Server first, there may be some servers where you can access to content without login, known as anonymous FTP.
- Client can start a conversation with server, upon requesting to download a file.
- The user can start different functions like upload, delete, rename, copy files, etc. on server.

FTP can work on different modes like Active and Passive modes. For more, you can refer to Difference between Active and Passive FTP.


User
File Transfer Protocol
User Interface
Control process
Data transfer process
Disk
Client
Control connection
TCP/IP
Data connection
Control process
Data transfer process
Disk
Server

Types of Connection in FTP

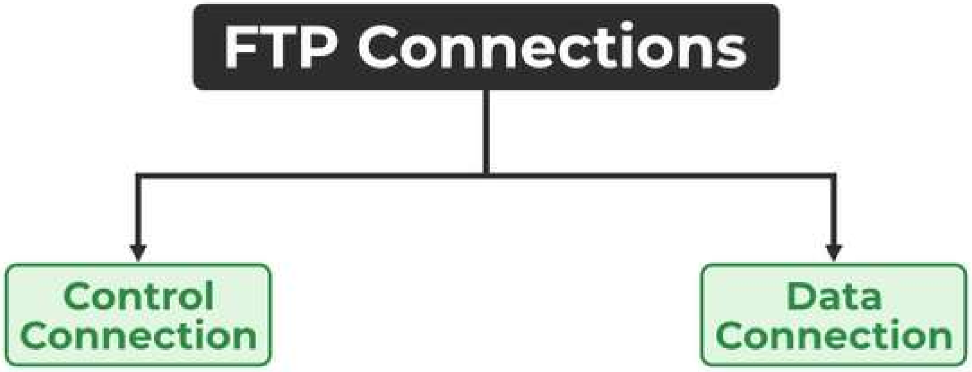
- Control Connection
- Data Connection

Control Connection

For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of a control connection. The control connection is initiated on port number 21.

Data connection

For sending the actual file, FTP makes use of a data connection. A data connection is initiated on port number 20.
FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.



FTP Session

When an FTP session is started between a client and a server, the client initiates a control TCP connection with the server side. The client sends control information over this. When the server receives this, it initiates a data connection to the client side. But the control connection remains active throughout the user session. As we know HTTP is stateless . But FTP needs to maintain a state about its user throughout the session.

FTP Clients

FTP works on a client-server model. The FTP client is a program that runs on the user's computer to enable the user to talk to and get files from remote computers. It is a set of commands that establishes the connection between two hosts, helps to transfer the files, and then closes the connection.

Some of the commands are:

> *get the filename(retrieve the file from the server)*
>
> *get the filename(retrieve multiple files from the server)*
>
> *ls(list files available in the current directory of the server)*

There are also built-in FTP programs, which makes it easier to transfer files and it does not require remembering the commands.

FTP Data Types

The data type of a file, which determines how the file is represented overall, is the first piece of information that can be provided about it. The FTP standard specifies the following four categories of data:

- **ASCII:** Describes an ASCII text file in which each line is indicated by the previously mentioned type of end-of-line marker.
- **EBCDIC:** For files that use IBM's EBCDIC character set, this type is conceptually identical to ASCII.
- **Image:** This is the "black box" mode I described earlier; the file has no formal internal structure and is transferred one byte at a time without any processing.
- **Local:** Files containing data in logical bytes with a bit count other than eight can be handled by this data type.

FTP Replies

Some of the FTP replies are:

- 200 - Command okay.
- 530 - Not logged in.
- 331 - User name okay, need a password.

- 221 - Service closing control connection.
- 551 - Requested action aborted: page type unknown.
- 502 - Command not implemented.
- 503 - Bad sequence of commands.
- 504 - Command not implemented for that parameter.

Characteristics of FTP

- FTP uses TCP as a transport layer protocol.
- It is good for simple file transfers, such as during boot time.
- Errors in the transmission (lost packets, checksum errors) must be handled by the TFTP server.
- It uses only one connection through well-known port 69.
- TFTP uses a simple lock-step protocol (each data packet needs to be acknowledged). Thus the throughput is limited.

FTP's Security Issues

- Information could not go across a secure tunnel since FTP was not intended to do so. Thus, encryption is not present. A hacker would not need to struggle with encryption to access or alter data that is usable if they could intercept an FTP transaction.
- Even with FTP cloud storage, data can still be intercepted and misused if the service provider's system is attacked.
- As a result, data sent via FTP is a target for spoofing, sniffing, brute force, and other types of attacks that move somewhat slowly. A hacker might examine an FTP transmission and try to take advantage of any flaws by simply port scanning.
- The fact that FTP uses clear-text passwords—passwords that haven't been encrypted—is one of its main security flaws. Put differently, "Jerry1992" appears exactly like "Jerry1992." The real password is hidden via an algorithm in more secure protocols. As a result, "Jerry1992" might appear as "dj18387saksng8937d9d8d7s6a8d89." Passwords like this are not secured by FTP, which makes them more easily cracked by malicious actors.

What is an FTP Port?

FTP operates using two ports:

- **Port 21:** As mentioned earlier this is where the commands are issued.
- **Port 20:** This is the special port required for data connection where the real transfer of file is made.

How to Change FTP Port Numbers

To change the default FTP port numbers, follow these steps:

- **Access Server Configuration:** Connect the control panel of your FTP server well as the FTP server configuration file used.
- **Modify the Port Number:** Find out the possible port settings from the configuration file. Alter the control port, default port is 21 and that of the data is 20.
- **Restart the FTP Service:** Finally once you have saved your changes you need to stop and restart the FTP service so that the new port settings can be implemented.
- **Update Client Settings:** Make certain that all the FTP clients that connect with the server are notified of the new port numbers.

Advantages of FTP

- File sharing also comes in the category of advantages of FTP in this between two machines files can be shared on the network.
- Speed is one of the main benefits of FTP.
- Since we don't have to finish every operation to obtain the entire file, it is more efficient.
- Using the username and password, we must log in to the FTP server. As a result, FTP might be considered more secure.
- We can move the files back and forth via FTP. Let's say you are the firm manager and you provide information to every employee, and they all reply on the same server.

Disadvantages of FTP

- File size limit is the drawback of FTP only 2 GB size files can be transferred.
- More then one receivers are not supported by FTP.
- FTP does not encrypt the data this is one of the biggest drawbacks of FTP.
- FTP is unsecured we use login IDs and passwords making it secure but they can be attacked by hackers.

Difference Between FTP and SFTP

FTP	SFTP
It stands for File Transfer Protocol.	It stands for Secure File Transfer Protocol.
In FTP, secure channel is not provided to transfer the files between the hosts.	In SFTP, a secure channel is provided to transfer the files between the hosts.
It usually runs on port no-21.	It usually runs on port no-22.
It does not encrypt the data before sending	It encrypted data before sending.
It makes uploading and downloading of files without any security.	It maintains full security of the data by using SSH keys.

FTP Security Challenges

FTP was not designed with security in mind, leading to several vulnerabilities:

- **Lack of Encryption:** This is because data such as usernames and passwords are transmitted without encryption and hence easily vulnerable to different attacks.
- **Vulnerabilities to Attacks:** FTP transmissions are vulnerable to attacks such as spoofing, sniffing, brute force , and the likes are slow attacks. They suggested that the data can be intercepted and changed easily by hackers .
- **Clear-Text Passwords:** Unfortunately, FTP client authentication employs non encrypted passwords, which makes them vulnerable to hacking.

Conclusion

FTP is still a powerful and effective method for transferring files between systems and still prevails in cases of transferring large files, and in the course of automated systems. Nevertheless, it does not come with security enhancements making it fairly inadequate for sensitive information exchange. In the case of transfers, safer modes like SFTP or FTPS should be encouraged since they make transfers secure. Hence, despite these drawbacks, FTP remains useful to this day since it is simple and stabilized.

Comment More info Advertise with us

Next Article

Basics of Wi-Fi

Similar Reads

1. Protocols in Application Layer
2. Application Layer Protocols in TCP/IP
3. What is Anonymous FTP (File Transfer Protocol)?
4. Application Layer in OSI Model
5. HTTP Full Form - Hypertext Transfer Protocol
6. Wireless Application Protocol
7. SFTP File Transfer Protocol

Asynchronous Transfer Mode (ATM) in Computer Network

Last Updated : 02 Nov, 2021

Why ATM networks?

1. Driven by the integration of services and performance requirements of both telephony and data networking: "broadband integrated service vision" (B-ISON).
2. Telephone networks support a single quality of service and are expensive to boot.
3. Internet supports no quality of service but is flexible and cheap.
4. ATM networks were meant to support a range of service qualities at a reasonable cost- intended to subsume both the telephone network and the Internet.

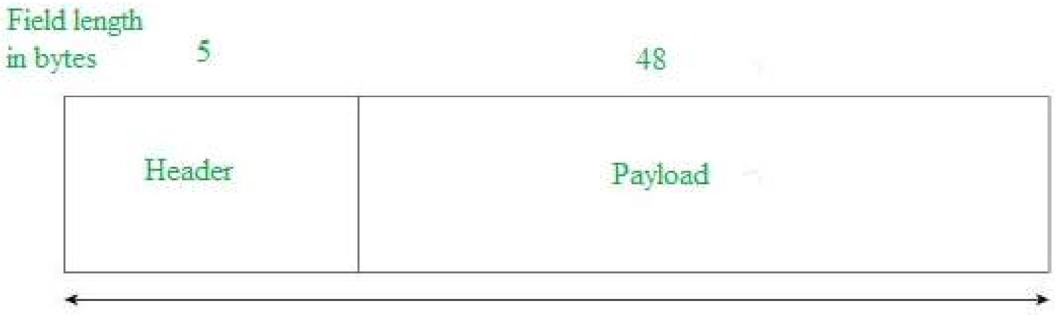
Asynchronous Transfer Mode (ATM):
It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.

ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching. *Each cell is 53 bytes long* - 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.

Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic. Thus it can carry multiple types of traffic with **end-to-end** quality of service. ATM is independent of a transmission medium, they may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems. ATM networks use "Packet" or "cell" Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking.

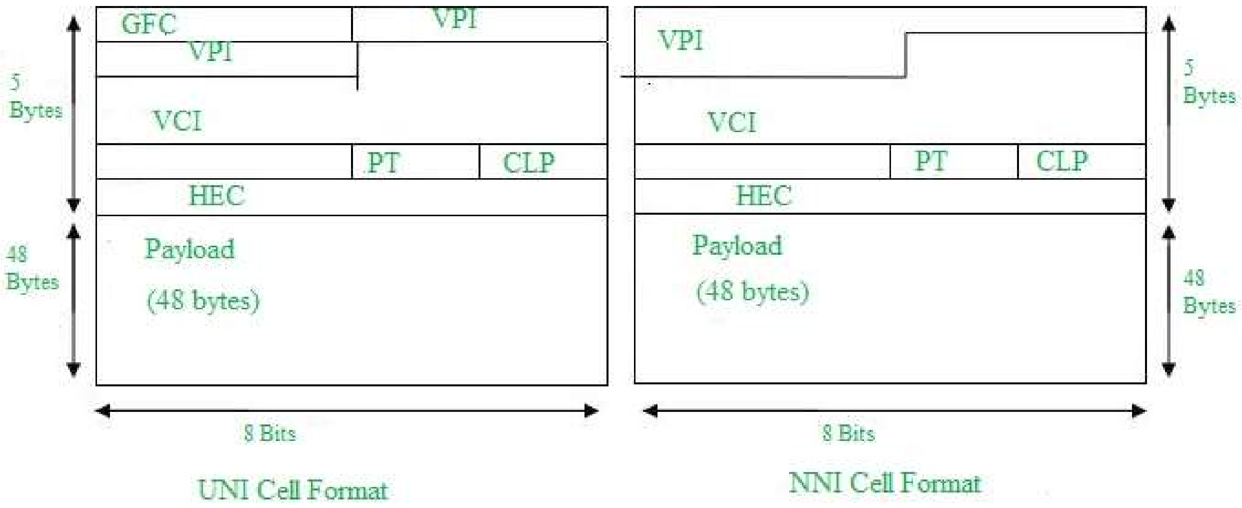
ATM Cell Format -

As information is transmitted in ATM in the form of fixed-size units called **cells**. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



ATM Cell Format

Asynchronous Transfer Mode can be of two format types which are as follows:


GFC
VPI
VPI
VCI
PT
CLP
HEC
Payload
(48 bytes)
5 Bytes
48 Bytes
8 Bits
UNI Cell Format
VPI
VCI
PT
CLP
HEC
Payload
(48 bytes)
5 Bytes
48 Bytes
8 Bits
NNI Cell Format

1. **UNI Header:** This is used within private networks of ATMs for communication between ATM endpoints and ATM switches. It includes the Generic Flow Control (GFC) field.

2. **NNI Header:** is used for communication between ATM switches, and it does not include the Generic Flow Control(GFC) instead it includes a Virtual Path Identifier (VPI) which occupies the first 12 bits.

Working of ATM:

ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not rout the cells to a particular virtual circuit. In case of major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.

Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.

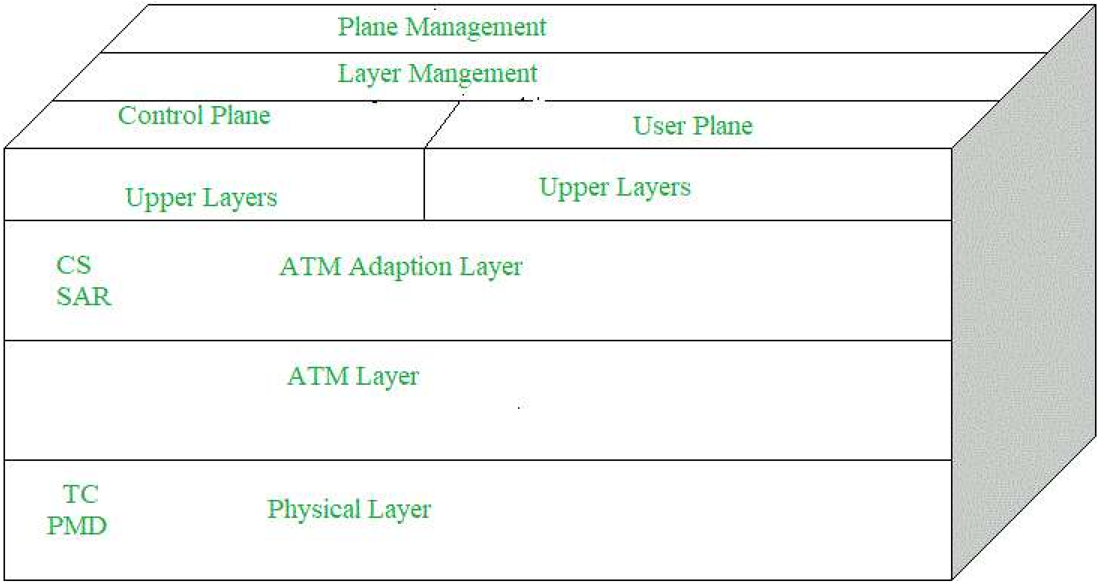
ATM vs DATA Networks (Internet) -

- ATM is a "virtual circuit" based: the path is reserved before transmission. While Internet Protocol (IP) is connectionless and end-to-end resource reservations are not possible. RSVP is a new signaling protocol on the internet.

- ATM Cells: Fixed or small size and Tradeoff is between voice or data. While IP packets are of variable size.

- Addressing: ATM uses 20-byte global NSAP addresses for signaling and 32-bit locally assigned labels in cells. While IP uses 32-bit global addresses in all packets.

ATM Layers:


Plane Management
Layer Mangement
Control Plane
User Plane
Upper Layers
Upper Layers
CS
SAR
ATM Adaption Layer
ATM Layer
TC
PMD
Physical Layer

1. **ATM Adaption Layer (AAL) -**
   It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells.

2. **Physical Layer -**
   It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer. The main functions are as follows:
   - It converts cells into a bitstream.
   - It controls the transmission and receipt of bits in the physical medium.
   - It can track the ATM cell boundaries.
   - Look for the packaging of cells into the appropriate type of frames.

3. **ATM Layer -**
   It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.

ATM Applications:

1. **ATM WANs -**
   It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.
2. **Multimedia virtual private networks and managed services -**
   It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.
3. **Frame relay backbone -**
   Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internetworking services.
4. **Residential broadband networks -**
   ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.

5. **Carrier infrastructure for telephone and private line networks -** To make more effective use of SONET/SDH fiber infrastructures by building the ATM infrastructure for carrying the telephonic and private-line traffic.

Comment More info Advertise with us

Next Article

Asynchronous Transfer Mode (ATM) in Computer Network

Similar Reads

1. Multiple Access Protocols in Computer Network
2. CATA protocol in Computer Network
3. Protocol and Standard in Computer Networks
4. Socket in Computer Network
5. Commonly asked Computer Networks Interview Questions | Set 1
6. How data is tranferred over computer network?
7. Basic Characteristics of Computer Networks
8. Controlled Access Protocols in Computer Network
9. TCP/IP in Computer Networking
10. Computer Networks | Set 8

Corporate & Communications Address:

A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Dynamic Host Configuration Protocol (DHCP)

Last Updated : 27 Dec, 2024

Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones, and printers) on a network. Instead of manually configuring each device with an IP address, DHCP allows devices to connect to a network and receive all necessary network information, like IP address, subnet mask, default gateway, and DNS server addresses, automatically from a DHCP server.

This makes it easier to manage and maintain large networks, ensuring devices can communicate effectively without conflicts in their network settings. DHCP plays a crucial role in modern networks by simplifying the process of connecting devices and managing network resources efficiently.

What is DHCP?

DHCP stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. DHCP helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as desktops, laptops, cellphones, etc. is an application layer protocol that is used to provide:

```
Subnet Mask (Option 1 - e.g., 255.255.255.0)
Router Address (Option 3 - e.g., 192.168.1.1)
DNS Address (Option 6 - e.g., 8.8.8.8)
Vendor Class Identifier (Option 43 - e.g.,
'unifi' = 192.168.1.9 ##where unifi = controller)
```

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

Why Do We Use DHCP?

DHCP helps in managing the entire process automatically and centrally. DHCP helps in maintaining a unique IP Address for a host using the server. DHCP servers maintain information on TCP/IP configuration and provide configuration of address to DHCP-enabled clients in the form of a lease offer.

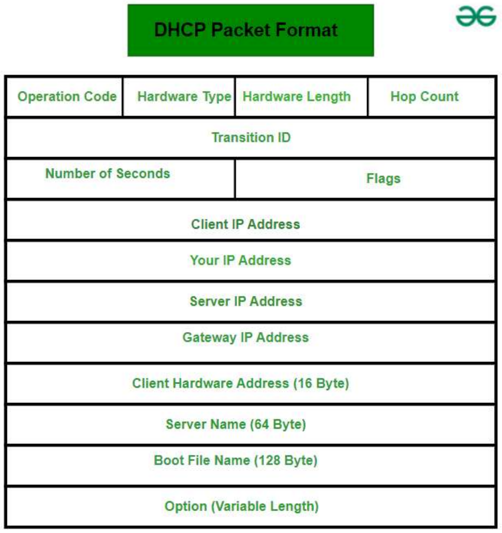
Components of DHCP

The main components of DHCP include:

- **DHCP Server:** DHCP Server is a server that holds IP Addresses and other information related to configuration.
- **DHCP Client:** It is a device that receives configuration information from the server. It can be a mobile, laptop, computer, or any other electronic device that requires a connection.
- **DHCP Relay:** DHCP relays basically work as a communication channel between DHCP Client and Server.
- **IP Address Pool:** It is the pool or container of IP Addresses possessed by the DHCP Server. It has a range of addresses that can be allocated to devices.
- **Subnets:** Subnets are smaller portions of the IP network partitioned to keep networks under control.
- **Lease:** It is simply the time that how long the information received from the server is valid, in case of expiration of the lease, the tenant must have to re-assign the lease.
- **DNS Servers:** DHCP servers can also provide DNS (Domain Name System) server information to DHCP clients, allowing them to resolve domain names to IP addresses.
- **Default Gateway:** DHCP servers can also provide information about the default gateway, which is the device that packets are sent to when the destination is outside the local network.
- **Options:** DHCP servers can provide additional configuration options to clients, such as the subnet mask, domain name, and time server information.

- **Renewal:** DHCP clients can request to renew their lease before it expires to ensure that they continue to have a valid IP address and configuration information.
- **Failover:** DHCP servers can be configured for failover, where two servers work together to provide redundancy and ensure that clients can always obtain an IP address and configuration information, even if one server goes down.
- **Dynamic Updates:** DHCP servers can also be configured to dynamically update DNS records with the IP address of DHCP clients, allowing for easier management of network resources.
- **Audit Logging:** DHCP servers can keep audit logs of all DHCP transactions, providing administrators with visibility into which devices are using which IP addresses and when leases are being assigned or renewed.

DHCP Packet Format


DHCP Packet Format
Operation Code
Hardware Type
Hardware Length
Hop Count
Transition ID
Number of Seconds
Flags
Client IP Address
Your IP Address
Server IP Address
Gateway IP Address
Client Hardware Address (16 Byte)
Server Name (64 Byte)
Boot File Name (128 Byte)
Option (Variable Length)

DHCP Packet Format

- **Hardware Length:** This is an 8-bit field defining the length of the physical address in bytes. e.g for Ethernet the value is 6.
- **Hop count:** This is an 8-bit field defining the maximum number of hops the packet can travel.

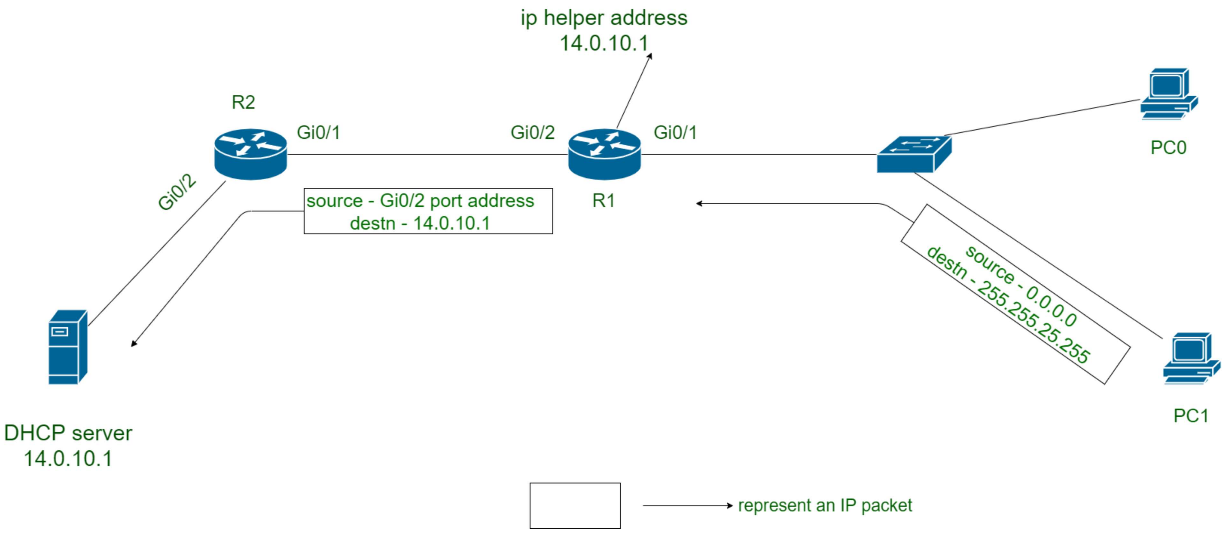
- **Transaction ID:** This is a 4-byte field carrying an integer. The transcation identification is set by the client and is used to match a reply with the request. The server returns the same value in its reply.
- **Number of Seconds:** This is a 16-bit field that indicates the number of seconds elapsed since the time the client started to boot.
- **Flag:** This is a 16-bit field in which only the leftmost bit is used and the rest of the bit should be set to os. A leftmost bit specifies a forced broadcast reply from the server. If the reply were to be unicast to the client, the destination. IP address of the IP packet is the address assigned to the client.
- **Client IP Address:** This is a 4-byte field that contains the client IP address . If the client does not have this information this field has a value of 0.
- **Your IP Address:** This is a 4-byte field that contains the client IP address. It is filled by the server at the request of the client.
- **Server IP Address:** This is a 4-byte field containing the server IP address. It is filled by the server in a reply message.
- **Gateway IP Address:** This is a 4-byte field containing the IP address of a routers. IT is filled by the server in a reply message.
- **Client Hardware Address:** This is the physical address of the client .Although the server can retrieve this address from the frame sent by the client it is more efficient if the address is supplied explicity by the client in the request message.
- **Server Name:** This is a 64-byte field that is optionally filled by the server in a reply packet. It contains a null-terminated string consisting of the domain name of the server. If the server does not want to fill this filed with data, the server must fill it with all 0s.
- **Boot Filename:** This is a 128-byte field that can be optionally filled by the server in a reply packet. It contains a null- terminated string consisting of the full pathname of the boot file. The client can use this path to retrieve other booting information. If the server does not want to fill this field with data, the server must fill it with all 0s.

- **Options:** This is a 64-byte field with a dual purpose. IT can carry either additional information or some specific vendor information. The field is used only in a reply message. The server uses a number, called a magic cookie, in the format of an IP address with the value of 99.130.83.99. When the client finishes reading the message, it looks for this magic cookie. If present the next 60 bytes are options.

Working of DHCP

DHCP works on the Application layer of the **UDP Protocol**. The main task of DHCP is to dynamically assigns IP Addresses to the Clients and allocate information on TCP/IP configuration to Clients. For more, you can refer to the Article Working of DHCP.

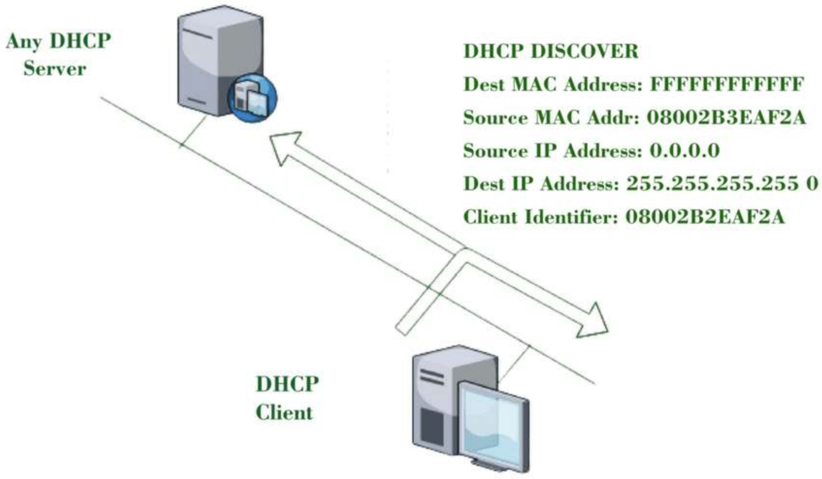
The DHCP **port number** for the server is 67 and for the client is 68. It is a client-server protocol that uses UDP services. An IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called the DORA process, but there are 8 DHCP messages in the process.


ip helper address
14.0.10.1
R2
Gi0/1
Gi0/2
Gi0/1
PC0
Gi0/2
source - Gi0/2 port address
destn - 14.0.10.1
R1
source - 0.0.0.0
destn - 255.255.25.255
PC1
DHCP server
14.0.10.1
represent an IP packet

Working of DHCP

The 8 DHCP Messages

1. DHCP Discover Message: This is the first message generated in the communication process between the server and the client. This message is generated by the Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long.

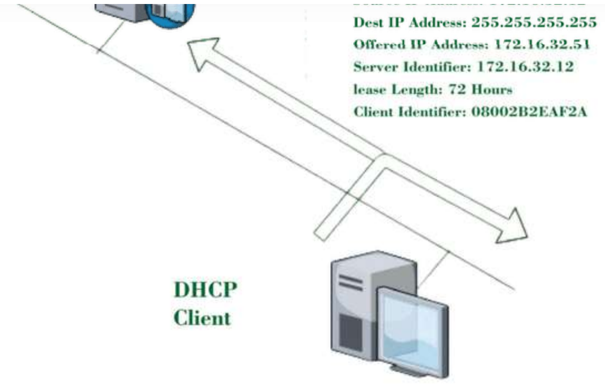


DHCP DISCOVER
Dest MAC Address: FFFFFFFFFFFF
Source MAC Addr: 08002B3EAF2A
Source IP Address: 0.0.0.0
Dest IP Address: 255.255.255.255 0
Client Identifier: 08002B2EAF2A

DHCP Discover Message

As shown in the figure, the source MAC address (client PC) is 08002B2EAF2A, the destination MAC address(server) is FFFFFFFFFFFF, the source IP address is 0.0.0.0(because the PC has had no IP address till now) and the destination IP address is 255.255.255.255 (IP address used for broadcasting). As they discover message is broadcast to find out the DHCP server or servers in the network therefore broadcast IP address and MAC address is used.

2. DHCP Offers A Message: The server will respond to the host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by the server. The size of the message is 342 bytes. If there is more than one DHCP server present in the network then the client host will accept the first DHCP OFFER message it receives. Also, a server ID is specified in the packet in order to identify the server.

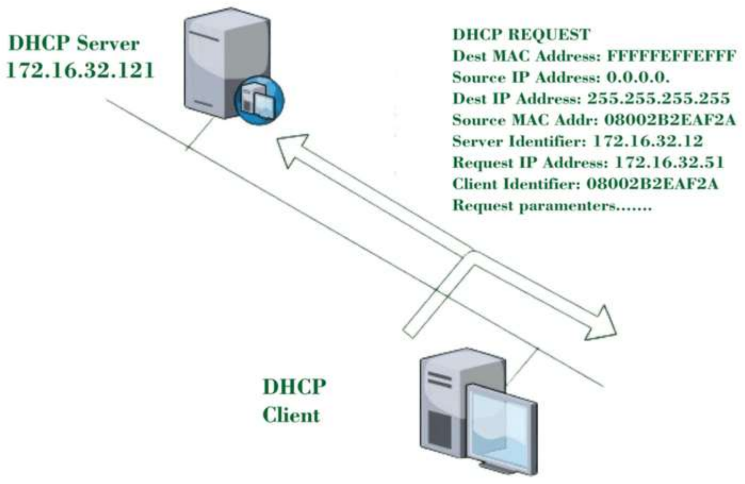

Dest IP Address: 255.255.255.255
Offered IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
lease Length: 72 Hours
Client Identifier: 08002B2EAF2A
DHCP Client

DHCP Offer Message

Now, for the offer message, the source IP address is 172.16.32.12 (server's IP address in the example), the destination IP address is 255.255.255.255 (broadcast IP address), the source MAC address is 00AA00123456, the destination MAC address is 00:11:22:33:44:55 (client's MAC address). Here, the offer message is broadcast by the DHCP server therefore destination IP address is the broadcast IP address and destination MAC address is 00:11:22:33:44:55 (client's MAC address)and the source IP address is the server IP address and the MAC address is the server MAC address.

Also, the server has provided the offered IP address 192.16.32.51 and a lease time of 72 hours(after this time the entry of the host will be erased from the server automatically). Also, the client identifier is the PC MAC address (08002B2EAF2A) for all the messages.

3. DHCP Request Message: When a client receives an offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with the same IP address. If there is no reply from another host, then there is no host with the same TCP configuration in the network and the message is broadcasted to the server showing the acceptance of the IP address. A Client ID is also added to this message.

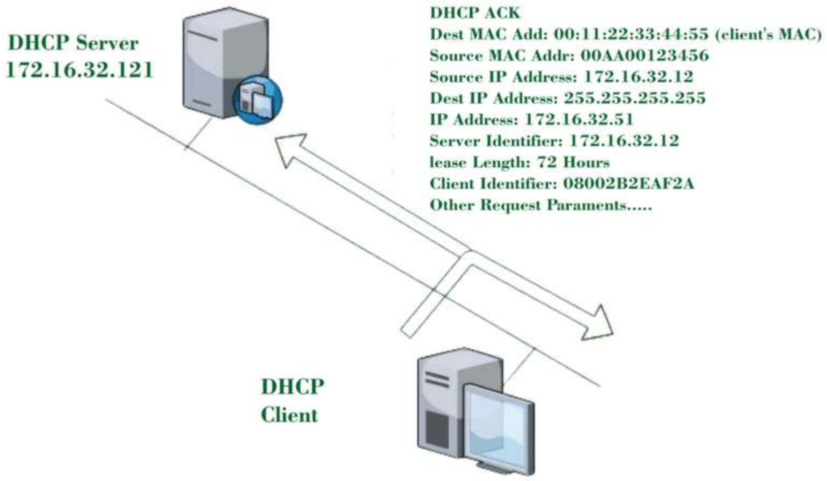

DHCP Server
172.16.32.121
DHCP REQUEST
Dest MAC Address: FFFFFEFFEFFF
Source IP Address: 0.0.0.0.
Dest IP Address: 255.255.255.255
Source MAC Addr: 08002B2EAF2A
Server Identifier: 172.16.32.12
Request IP Address: 172.16.32.51
Client Identifier: 08002B2EAF2A
Request paramenters.......
DHCP
Client

DHCP Request Message

Now, the request message is broadcast by the client PC therefore source IP address is 0.0.0.0(as the client has no IP right now) and destination IP address is 255.255.255.255 (the broadcast IP address) and the source MAC address is 08002B2EAF2A (PC MAC address) and destination MAC address is FFFFFFFFFFFF.

Note - This message is broadcast after the ARP request broadcast by the PC to find out whether any other host is not using that offered IP. If there is no reply, then the client host broadcast the DHCP request message for the server showing the acceptance of the IP address and Other TCP/IP Configuration.

4. DHCP Acknowledgment Message: In response to the request message received, the server will make an entry with a specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by the server.


DHCP Server
172.16.32.121
DHCP ACK
Dest MAC Add: 00:11:22:33:44:55 (client's MAC)
Source MAC Addr: 00AA00123456
Source IP Address: 172.16.32.12
Dest IP Address: 255.255.255.255
IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
lease Length: 72 Hours
Client Identifier: 08002B2EAF2A
Other Request Paraments.....
DHCP
Client

Now the server will make an entry of the client host with the offered IP address and lease time. This IP address will not be provided by the server to any other host. The destination MAC address is 00:11:22:33:44:55 (client's MAC address) and the destination IP address is 255.255.255.255 and the source IP address is 172.16.32.12 and the source MAC address is 00AA00123456 (server MAC address).

5. DHCP Negative Acknowledgment Message: Whenever a DHCP server receives a request for an IP address that is invalid according to the scopes that are configured, it sends a DHCP Nak message to the client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to the client.

6. DHCP Decline: If the DHCP client determines the offered configuration parameters are different or invalid, it sends a DHCP decline message to the server. When there is a reply to the gratuitous ARP by any host to the client, the client sends a DHCP decline message to the server showing the offered IP address is already in use.

7. DHCP Release: A DHCP client sends a DHCP release packet to the server to release the IP address and cancel any remaining lease time.

8. DHCP Inform: If a client address has obtained an IP address manually then the client uses DHCP information to obtain other local configuration parameters, such as domain name. In reply to the DHCP inform message, the DHCP server generates a DHCP ack message with a local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

Note - All the messages can be unicast also by the DHCP relay agent if the server is present in a different network.

Security Considerations for Using DHCP

To make sure your DHCP servers are safe, consider these DHCP security issues:

- **Limited IP Addresses** : A DHCP server can only offer a set number of IP addresses. This means attackers could flood the server with requests, causing essential devices to lose their connection.
- **Fake DHCP Servers** : Attackers might set up fake DHCP servers to give out fake IP addresses to devices on your network.
- **DNS Access** : When users get an IP address from DHCP, they also get DNS server details. This could potentially allow them to access more data than they should. It's important to restrict network access, use firewalls, and secure connections with VPNs to protect against this.

Protection Against DHCP Starvation Attack

A DHCP starvation attack happens when a hacker floods a DHCP server with requests for IP addresses. This overwhelms the server, making it unable to assign addresses to legitimate users. The hacker can then block access for authorized users and potentially set up a fake DHCP server to intercept and manipulate network traffic, which could lead to a man-in-the-middle attack.

Reasons Why Enterprises Must Automate DHCP?

Automating your DHCP system is crucial for businesses because it reduces the time and effort your IT team spends on manual tasks. For instance, DHCP-related issues like printers not connecting or subnets not working with the main network can be avoided automatically.

Automated DHCP also allows your operations to grow smoothly. Instead of hiring more staff to handle tasks that automation can manage, your team can focus on other important areas of business growth.

Advantages

- Centralized management of IP addresses.
- Centralized and automatedTCP/IP configuration .
- Ease of adding new clients to a network.
- Reuse of IP addresses reduces the total number of IP addresses that are required.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable devices that move to different locations on a wireless network.
- Simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client.
- The DHCP protocol gives the network administrator a method to configure the network from a centralized area.
- With the help of DHCP, easy handling of new users and the reuse of IP addresses can be achieved.

Disadvantages

- IP conflict can occur.
- The problem with DHCP is that clients accept any server. Accordingly, when another server is in the vicinity, the client may connect with this server, and this server may possibly send invalid data to the client.
- The client is not able to access the network in absence of a DHCP Server.
- The name of the machine will not be changed in a case when a new IP Address is assigned.

Conclusion

In conclusion, DHCP is a technology that simplifies network setup by automatically assigning IP addresses and network configurations to devices. While DHCP offers convenience, it's important to manage its security carefully. Issues such as IP address exhaustion, and potential data access through DNS settings highlight the need for robust security measures like firewalls and VPNs to protect networks from unauthorized access and disruptions. DHCP remains essential for efficiently managing network connections while ensuring security against potential risks.

Comment More info Advertise with us

Next Article

DHCP Starvation Attack

Similar Reads

1. Working of Dynamic Host Configuration Protocol
2. Dynamic Host Configuration Protocol (DHCP) vs Static IP Assignment
3. DHCP Server Configuration in Cisco
4. IPCONFIG Full Form - Internet Protocol configuration
5. Network Control Protocol (NCP)
6. Bandwidth Allocation Control Protocol (BACP)
7. ARP Protocol Packet Format
8. Bandwidth Allocation Protocol (BAP)
9. Packet Tracer to Configure DHCP On a Wireless Router
10. Uses of Configuration Register in Cisco Router

GeeksforGeeks
Sanchhaya Education Private Limited

Corporate & Communications Address:
A-143, 7th Floor, Sovereign Corporate
Tower, Sector- 136, Noida, Uttar Pradesh
(201305)

Registered Address:
K 061, Tower K, Gulshan Vivante
Apartment, Sector 137, Noida, Gautam